SANS Institute
InfoSec Reading Room

IDS File Forensics

Attackers usually follow an attack framework in order to breach an organization's computer network infrastructure. In response, forensic analysts are tasked with identifying files, data and tools accessed during a breach. Attackers follow a systematic approach in order to compromise their targets that begins by gathering information and intelligence. After identifying technology and personnel, they direct their efforts to gaining access to the organization's internal systems by exploiting vulnerabilities or ...

An Overview to Forensic Enterprise Architecture Design

GIAC (GCFA) Gold Certification

Author: George Khalil, George@GeorgeKhalil.com
Advisor: Richard Carbone

Accepted:
(Date your final draft is accepted by your advisor)

Abstract

Attackers usually follow an attack framework in order to breach an organization's computer network infrastructure. In response, forensic analysts are tasked with identifying files, data and tools accessed during a breach. Attackers follow a systematic approach in order to compromise their targets that begins by gathering information and intelligence. After identifying technology and personnel, they direct their efforts to gaining access to the organization's internal systems by exploiting vulnerabilities or through spear-phishing. Once the shellcode or malware has executed, it downloads additional components to provide the attacker with the necessary tools to move laterally across the organization and escalates his privileges. The attacker then extends this by collecting and exfiltrating confidential data. Each time a file is created or transferred across the network a detectable forensic signature is left behind. Even memory resident malware must exist as a file or traverse the network prior to being loaded into memory. Advanced persistent threat (APT) agents typically traverse the enterprise infrastructure during their attack and subsequent exfiltration activities. The design of a forensically sound infrastructure permits the identification of current and past malicious communications while network intelligence-gathering methods seek to create an enterprise-wide forensic view to identify the extent of a breach. Early detection of threats requires proper placement of Intrusion detection and prevention systems. File analysis, DLP, Syslog, NetFlow logging and behavior analysis provide visibility of enterprise wide activities from the perspective of multiple systems.

1. Introduction

The forensic community has developed an eight-step methodology to identify each step used against an organization's systems and network as illustrated in publication NIST SP800-86 (NIST.gov, 2015). As attackers work through the various phases of the attack, they leave traceable and detectable events. Attackers typically start by creating a profile for their target. This is done by gathering all available data regarding the organization through publically accessible resources, including its public figures, leadership, and staff including a list of who may have access to privileged data. Publicly accessible networks, Internet connectivity and websites are identified and documented in the target's profile. Employee skillsets posted on job sites, resumes, and discussion boards are used to identify products and vendors deployed across the target organization. Other publicly available information includes anything related to identify technologies, staff skillsets and exposed vulnerabilities in the organization's Internet-facing infrastructure. The next phase of intelligence gathering moves on to identifying current projects, researching employees and executive staff to prepare a social engineering spear-phishing campaign.

The attacker then redirects their efforts targeting exposed and vulnerable infrastructure. The current standard of security practice adopted by most organizations is to harden their perimeter defenses thereby reducing the exposed vulnerable attack surface forcing attackers to target the organization through its internal infrastructure. Advanced persistent threat (APT) analysis from TrendMicro noted that the human element is key for an attacker to gain access to an organization's internal systems (TrendMicro, 2012). Their analysis, performed in 2011 analyzed 20 of the largest data breaches, confirmed that protection via perimeter defense no longer works due to an increasingly mobile and connected workforce. Sophisticated attackers are targeting individuals within organizations using custom spear-phishing emails containing custom malware to avoid detection. Attackers use the information collected during this reconnaissance phase to convince the employee that the email is from a legitimate source and contains work-related files (Hipolito, 2014). The custom malware usually has a decoy front-end document to reduce the likelihood of the victim becoming aware of the malware payload.

Author Name, email@address

Once the custom malware is executed, it initiates an outbound connection back to the attackers' command and control servers, bypassing all inbound filtering and perimeter protection mechanisms and granting the attacker generous access to the internal infrastructure. According to McAfee's Diary of a "RAT" (for "Remote Access Tool"), APT remote access tools only make outbound connections; 83 percent use outbound ports 80 or 443 and are proxy compatible (Mcafee.com, 2015). APTs rely on per-organization custom malware to avoid anti-virus, IDS/IPS signature detection, MD5 hashes, and filename matching (Mcafee.com, 2015). Once the attacker establishes persistence on the initial point of compromise, they quickly discover the organization's infrastructure, personnel and security mechanisms. The attacker may deploy additional malware after the initial compromise to extend their reach within the organization (moving laterally).

Once internal intelligence gathering is done, the attacker moves on to gain enterprise-wide persistence, the goal being to attain the highest level of privilege and access protected information. Collected data is then exfiltrated and transmitted outside the organization using a variety of methods. Attackers typically create a large archive containing the data of interest and transmit it using HTTP or HTTPS, DNS, or FTP. Advanced attackers prefer HTTP or HTTPS traffic to blend their malicious activities with standard corporate web traffic and intermittently with DNS traffic.

Attackers typically identify personnel with access to sensitive information and target them using common management tools such as Windows management instrument "WMI" to identify open files along with the operating system and applications showing recent file usage. This technique allows the attacker to find high-value data based on frequent user access to important files (TrendMicro Global R&D Center, 2015).

Each phase of an attack along the lines of the one just described above leaves a detectable forensic event. Defenders and forensic analysts can use these artifacts to identify the extent and scope of the breach. The attacker's activities leave behind logs of what port, service and application were utilized during external and internal reconnaissance. IDS/IPS infrastructure and network and system logs can provide critical indicators of reconnaissance-based activities and possibly indicators of compromise (IOCs). Network, database and web application enumeration leave behind artifacts in

network security and monitoring infrastructure along with their server logs. Attackers' spear-phishing exist within the organization's email system; an antivirus scanning system and network flow monitoring infrastructure can track the source and the destination of their malicious content. Once the attacker gains access to an internal system, the outbound communication with the command and control infrastructure is logged through the network traffic monitor, firewall and Internet-filtering infrastructure. Attackers leave behind artifacts during lateral movement, discovery, access and compromise. Data exfiltration takes places through a variety of protocols, which must typically carry large outbound payloads, leaving behind a sizable and detectable event.

Network forensics is critical in detecting attackers through live forensics and post-breach forensic analysis. Attackers gain access to systems and possibly infrastructure. The logging infrastructure must be kept in a separate secure environment to protect the integrity of the logs. Network intrusion detection and prevention systems and network logging systems play a key role in tracking each phase of an attack.

TrendMicro's malicious data breach diagram (shown in Figure 1) illustrates the attack process and opportunities to identify detection and logging zones.

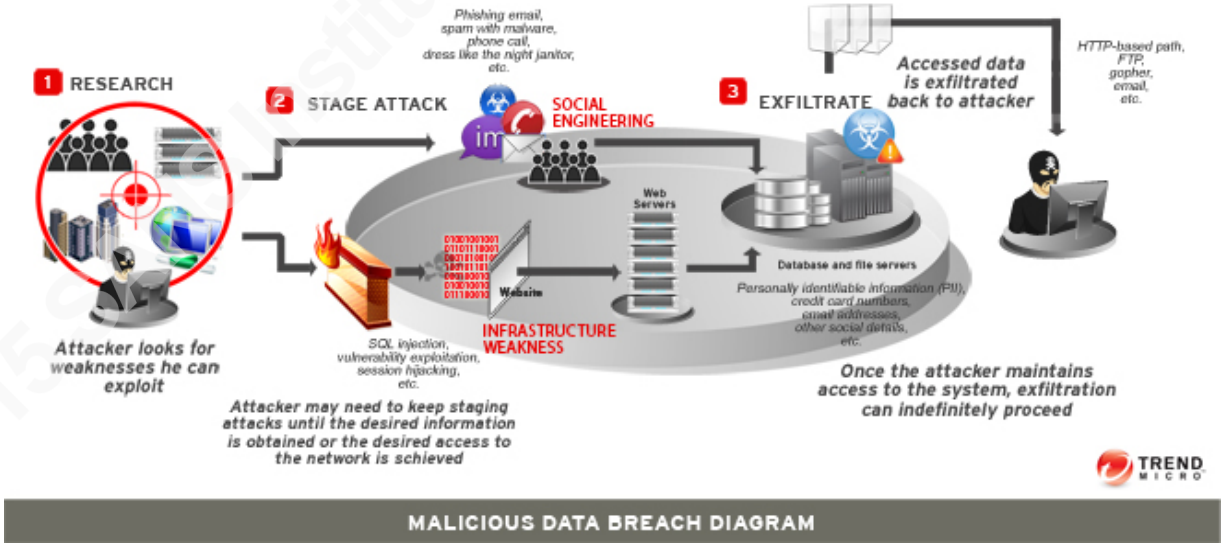

Figure 1. Malicious data breach diagram (TrendMicro Global R&D Center, 2015).

Each stage of an attack presents an opportunity to contain the users or systems within a protected enclave. Connectivity between the users, infrastructure, and

confidential data is an ideal location for implementing IDS/IPS and extensive communication-based logging. Open source and commercial IDS/IPS products such as Snort, Suricata and Bro offer the standard signature matching alerting and blocking feature. However, with APTs, signature matching has limited value due to the predominant use of zero-day and custom malware. Suricata offers filename matching and MD5 hash white and black listing but which are ineffective at identifying custom malicious files. In contrast, Suricata is extremely effective at identifying known confidential data movement between internal systems. Organizations can deploy a host-based IPS to increase visibility into sensitive data at the system level and deploy network-based IDS systems to increase visibility throughout the network. In addition to deploying IDS file-matching capabilities, Suricata offers file-size and extension-based signatures. Organizations can detect and block APT activities by detecting and blocking large file transfers that exceed normal operational baselines (Suricata-ids.org, 2015).

In addition to alerting and blocking, IDS and IPS systems provide the capability for extracting files from network data streams. *File carving* provides significant forensic benefits in detecting malware staging, data collection and exfiltration. Suricata can be configured to detect file-based (Magic) signatures and set up to provide alerts (for example, using alert rules) based on file extension or signatures. Extracted files can be stored and scanned using antivirus software, data loss prevention (DLP) tools or file-matching tools to identify critical files being exfiltrated from the network. The files alone could alert the organization to confidential data movement in preparation for data exfiltration. In addition to detection, file carving can also provide traceable forensic events for some of the phases of the breach. IDS and IPS systems provide alerting, logging and file extraction features that could be used to identify compromised users, workstations, servers and applications.

Suricata 2.1 beta2 introduced Simple Mail Transfer Protocol (STP) file extraction in addition to existing HTTP file extraction. Bro IDS also offers HTTP, FTP, SMTP, and IRC (Internet Relay Chat) file extraction capabilities (Randall, 2013). SSL encrypted traffic remains a challenge for open-source IDS; as an alternative, Suricata and Bro offer options to record all SSL certificates exchanged during SSL sessions. Alternative

strategies exist to deploy proxy servers such as Squid to intercept, log, and decrypt SSL traffic. The decrypted traffic can be further inspected using an open source IDS/IPS.

Network logging tools such as Syslog, DNS, NetFlow, behavior analytics, IP reputation, honeypots, and DLP solutions provide visibility into the entire infrastructure. This visibility is important because signature-based systems are no longer sufficient for identifying the advanced attacker that relies heavily on custom malware and zero-day exploits (ISACA, 2013). Having knowledge of each host's communications, protocols, and traffic volumes as well as the content of the data in question is key to identifying zero-day and APT malware and agents. Data intelligence allows forensic analysis to identify anomalous or suspicious communications by comparing suspected traffic patterns against normal data communication behavioral baselines. Automated network intelligence and next-generation live forensics provide insight into network events and rely on analytical decisions based on known vs. unknown behavior taking place within a corporate network.

2. Forensic Network Design

Knowing the attackers' strategy empowers security professionals to apply appropriate security controls within their network. The forensic community developed a framework designed to identify attackers through each phase of the attack. Each phase also presents an opportunity to apply different tools to maximize the collection of data and increase the likelihood of more quickly detecting malicious activity. Table 1 illustrates the forensic framework and the corresponding attacker's activities.

Table 1. **The eight steps of the forensic framework (George Khalil; based on publication NIST SP800-86).**

Forensic Framework	Corresponding Attacker Activity
Verification	Gain and maintain access
System Description	Gain and maintain access, lateral movement
Evidence Acquisition	Acquire data, implant malware, spear phishing campaign, reconnaissance, and exploit payload deployment
Timeline Analysis	Identify attacker activity
Media and Artifact Analysis	Deploy malware, tools, collect and exfiltrate data
String or Byte Search	Identify attacker activity

Forensic Framework	Corresponding Attacker Activity
Data Recovery	Deploy malware, tools, collect and exfiltrate data
Reporting Results	Lessons Learned

Secure network design revolves around containing protected data within secure enclaves. This concept of compartmentalization promotes the creation of security zones with placement of IDS/IPS, Firewalls, and Network and Flow logging between the zones (Payment and Security Experts, Juniper, 2015). Servers, users and databases should have single choke points that allow strict application of security rules and logging. Automatic file extraction, automated scanning, and protected file and DLP is key to identifying an attacker during the early phases of an attack and in forensically tracing the steps of an attacker postmortem.

2.1. IDS/IPS Forensic Implementation

Intrusion detection and prevention systems (IDS/IPS) offer significant logging and alerting capabilities. Historically IDS/IPS systems have been used to alert and block intrusions; however, APT attack significantly reduced the effectiveness of most signature based security infrastructure. Combating APT requires the application of standard security tools in new ways. Forensic and behavior analysis is vital to identifying and detecting malicious activities. Suricata and Bro provide extensive next-generation open-source IDS/IPS features that can be configured to provide many of the requirements examined in the subsequent subsections.

2.1.1. Forensic File logging

Suricata provides extensive detection engines using protocol keywords, Perl Compatible Regular Expressions (PCRE), fast pattern matching using Suricata's payload inspection rule, filemagic, size naming, extension and MD5 checksumming (Suricata-ids.org, 2015). In addition to detecting malicious files and signatures, defenders should adapt their detection capabilities to identify the movement of protected data. For Suricata's file matching capabilities, modify its YAML configuration file format (Openinfosecfoundation.org, 2015) to enable logging and alerting. This task can be accomplished by adding the following lines to the configuration file:

Filename matching syntax: "filename:<secret>;"
File extension matching: "fileext:".zip";"
Filemagic: "filemagic:"executable for MS Windows";
File MD5: "filemd5:md5-blacklist"; or "filemd5:!md-whitelist;"
Filesize: "filesize:100;" or "filesize:>100;" (Lang, 2015)

Bro offers similar features to detect malicious file signatures. These features allow for the detection of unauthorized data movement and subsequent alerts to be sent to security professionals method of choice. Identifying secure file movement is critical to combating a sophisticated attacker. Its alert history can also provide postmortem forensic analysis to identify tools, executables and methodology used by attackers in addition to identifying the extent of the breach. Bro's alert output can be configured for a fast line-based alert log or a more detailed Extensible Event Format for further forensic review using tools such as *logstash*. Additional output reporting options such as Syslog, DNS, HTTP communications and dropped traffic are available along with a packet capture. Archiving logs and traffic allow for future network forensic review of network traffic (Openinfosecfoundation.org, 2015).

The IDS/IPS logs provide forensic analysts with the capability of verifying the occurrence of an incident. They also permit the identification of involved systems, tools and timeline of the breach. The recorded logs and network traffic capture allows for evidence acquisition and data recovery of the tools and malware used to execute the attack. Finally, IDS/IPS rich logging capabilities provide the data necessary to execute the full breadth of the forensic framework.

2.1.2. Forensic file carving and analysis

Suricata and Bro offer automated file carving features. File extraction and carving can be configured based on the direction of traffic flow to or from monitored servers. File carving scope can be defined by creating a match list based on filenames, file-based magic signature or file extensions. It can also store all files matching a specific HTTP transaction or all files from a TCP session or flow that triggered an alert.

Suricata's file carving options require two separate output modules in addition to a rule to trigger the file-saving action. The file extraction option can be enabled using the Waldo file option to prevent files from being overwritten as the .id sequence is reset:

```
- file-store:
    enabled: yes      # set to yes to enable
    log-dir: files    # directory to store the files
    force-magic: no   # force logging magic on all stored files
    force-md5: no     # force logging of md5 checksums
    waldo: file.waldo # waldo file to store the file_id across runs

- file-log:
      enabled: yes
      filename: files-json.log
      append: yes
      #filetype: regular # 'regular', 'unix_stream' or 'unix_dgram'
      force-magic: no   # force logging magic on all logged files
      force-md5: no     # force logging of md5 checksums
```

Once the file extraction options are set, a rule must be configured to trigger the event or a matching item. The Standard signature format can be used to match any option available to the IDS/IPS with the output of "filestore". This also permits the usage of file matching using size, MD5 hash, filename or file-based magic matching and extraction of the file that matches a given rule, as shown in the following example (Openinfosecfoundation.org, 2015):

```
alert http any any -> any any (msg:"FILE pdf detected"; filemagic:"PDF
document"; filestore; sid:3; rev:1;)
```

Once the files are extracted, they can be scanned using an antivirus program to identify known malicious files. Some products (such as OPSWAT's Metascan) offer multivendor scan engines that can be hosted onsite. The solution is similar to the functionality offered by VirusTotal. Organizations can protect their privacy by implementing onsite scanning deployment. Onsite deployments also provide continuous automated scanning using 1, 4, 8, 12, 16 or 30 vendor's engines (Opswat.com, 2015).

2.2. Network Forensics

Network equipment and security devices provide a wealth of information that can identify malicious traffic. Attackers attempt to obfuscate their tracks on the systems that

they compromise. However, as the vast majority of attackers are remote, this traffic must traverse the network to communicate with its command and control servers. As the attacker moves laterally across the victim's network and attempts to exfiltrate data, routers, switches, and firewalls provide remote logging capabilities that can alert and help identify the attacker. Deploying and securing remote logging infrastructure is crucial to an in-depth implementation of a thorough defense and is key to forensic analysis.

2.2.1. Network Logging Forensics

Networks, servers, and the vast majority of security devices offer varying levels of data exports to a remote Syslog server. Firewalls and routers can export network device and access list events to a Syslog server (Cisco.com, 2015). Suricata, Snort and Bro offer Syslog output options to export alerts and signature matches to remote servers for analysis. In addition to network and security infrastructure, servers, authentication, and identity management systems provide Syslog output capabilities. These extensive logging capabilities from the entire enterprise infrastructure provide forensic investigators with a broad view of both attacker and user activity across the enterprise network. Denied Access Lists provide Syslog evidence of network and service scans, infrastructure discovery and lateral movement (Liu, 2009). Authentication Syslog provides artifacts and evidence of a successful breach (Garbrecht, 2015); account creation and takeover as well large scale successful or failed authentication requests that confirm the presence of an intruder within an organization's infrastructure.

The collected logs provide a large volume of raw data due to the vast amount of data transmitted and user activity across modern organizations. Third-party log-parsing systems such as Splunk or Lancope's StealthWatch translate raw logs into measurable, easy-to-understand baselines that allow organizations to understand the normal volume of user authentications and failed logins, network traffic, and the average number of events generated during normal business operations. Understanding normal operations baselines provides the capability of identifying the standard user, system and network behavior.

Attackers work hard at blending in with normal web traffic, management tools and network protocols. In spite of these attempts, when a forensic analyst is provided raw system data and operational behavior baselines, the attacker no longer blends in as a

standard user or administrator. A customer does not access several hundred pages on a corporate website, and users and administrators do not attempt to connect to several hundred systems concurrently. Forensic artifacts from single systems do not provide that level of visibility into the scale of the attack, nor do they provide large-scale behavior baselines (Splunk.com, 2015).

2.2.2. Network Traffic Analysis

In addition to various Syslog traffic, routers and IDS/IPS systems provide additional forensic data through flow data and packet captures. *Flow data* provides headers of all network communications, including source, destination, ports, size, and time of the event that are critical for differentiating between an attacker's artifacts and the normal business operational baseline. Flow data should be collected from all routers within the infrastructure especially at the perimeter of secure zones (Payment and Security Experts, Juniper, 2015). Forensic intelligence software such as Lancope's StealthWatch collects data from multiple sources (including NetFlow) to provide network communication logs for successful and failed communications.

NetFlow is an alternative to full network traffic captures. Logging the network packet headers allows organizations to have forensic data and piece together the attacker's activities without requiring the massive storage required to retain all network communications. Having visibility into the attacker's methodology provides the forensic analyst with future IOCs in addition to providing insight into the skill, methodology, progression and tools used by the attackers. Having infrastructure-wide visibility allows organizations to identify the source, scope, target and breached data that the attacker was seeking. According to Lancope, "NetFlow is a critical ingredient in the recipe of how you defend your network against attacks" (Lancope.com, 2015).

NetFlow can provide organizations with the means to determine normal operational baselines on an unprecedented scale. Syslog data can provide event-driven baselines. However, NetFlow provides a much more granular level of detail, enabling insight into time-stamped user and machine traffic. The data contain protocol usage, frequency, and amount of data transferred. Baselines of host-to-host communication maps can be created using NetFlow records, with alerts set up if a host communicates

with an unknown destination. Tools such as NetFlow Auditor, NetFlow Scrutinizer, Lancope StealthWatch, Solar Winds and others provide interactive dashboards, baselines, alerts and search capabilities, allowing quick forensic triage-based capabilities to security professionals.

Figure 2 illustrates how NetFlow data baselines can provide a quick indicator of data exfiltration and abnormal traffic volumes.

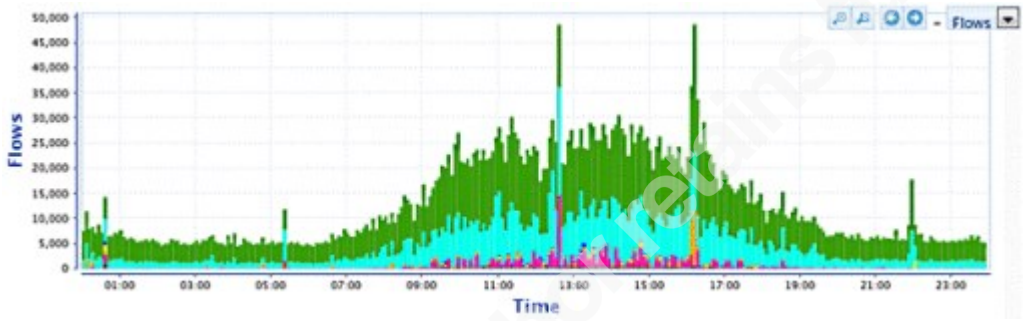

Figure 2. NetFlow depiction of data exfiltration and abnormal traffic volumes (shown by the higher bars in the center of the graph between 11:00 and 13:00 and between 15:00 and 17:00).

In addition to NetFlow data, Network TAPs and packet capture appliances can provide a complete copy of network communications. Data storage is a significant hurdle to full network packet capture and storage. Intrusion detection and prevention systems offer a compromise regarding packet captures. Suricata, for example, offers Pcap-logger output as an option, which is the capture of specific network traffic as based on the use of signatures to a Pcap file for future analysis (Suricata-ids.org, 2015). Having the raw network traffic allows forensic investigators to confirm if it is a false signature match or a true alert triggered by a malicious event.

Full packet capture allows forensic experts to extract network data of interest. Pcap file carving functionality allows for the extraction of files transferred from a monitored server. File extraction provides the means of creating custom detection signatures to identify a custom attack targeting the victim organization (GTKKlondike, 2015). The extracted malicious files can be used to determine the command and control servers, the attacker's communication channels, propagation techniques and additional

data that can assist in identifying malicious traffic inside the organization. Saved packet captures can be fed into multiple intrusion detection systems for additional analysis as well as provide a future replay of suspected malicious events.

IDS and IPS systems offer IP analysis and alerting features based on IP reputation. The sensor validates source and destination traffic against pre-configured or dynamic lists of bad hosts and known good and shared hosting providers (Openinfosecfoundation.org, 2015). The IP reputation lists are further broken down into categories such as command and control servers that can be used to create rules to alert or deny traffic matching IP category or IP addresses from the reputation lists. There are a multitude of organizations offering IP lists for emerging threats, including project Honey Pot, abuse.ch, Alien Vault, openbl.org, malwaregroup.com, autoshun.org and spamhaus.org. The deployment of an enterprise-wide network forensic architecture allows organizations to build security intelligence through the identification of known bad IP addresses and bad files. Although APT frequently uses custom malware, identifying known bad IP addresses and known bad files along with operational baselines can assist the organization in recognizing the presence of APT within their infrastructure.

Domain name servers play a critical role in building and maintaining a network forensic architecture. Logging, analyzing and retention of DNS requests allow organizations to perform DNS IP reputation checks to identify known bad or malicious traffic. Extracting DNS traffic through a network TAP can provide a packet capture file for future analysis and match against known offenders. Advanced attackers use DNS as a tunneling technique to communicate with command and control servers as well as to exfiltrate data through DNS requests where other methods of outbound communications may be restricted. Commercial products such as Infoblox Advanced DNS Protection (a datasheet on this is available at infoblox.com) offer DNS reputation and blocking services. The InfoBlox DNS firewall inspects all DNS requests and validates them against dynamically updated DNS reputation lists (Infoblox.com, 2015). Traffic is then logged to Syslog servers to create a forensic trail of events, as illustrated in Figure 3.

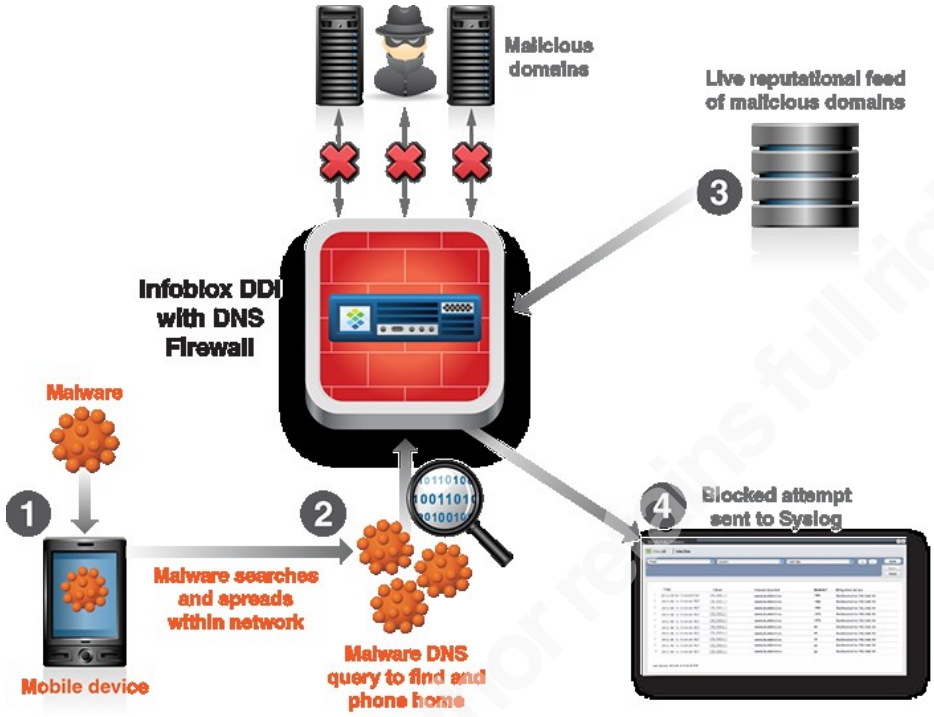

Figure 3. Elements of Infoblox.com Advanced DNS Protection (infoblox.com, 2015).

2.2.3. Network Traffic attack detection

In addition to behavior and normal operational baselines, the use of honeypots play a key role in setting traps and alerting forensic investigators to the presence of an advanced attacker. The general goal of forensic network design is to create as many possible artifacts that would provide evidence and indicators of a compromise once it occurs. Honeypots are typically designed to be stealth systems that do not provide any operational function to the organization but which provide easy prey for an intruder, and with minor modification allows an intruder's activity to be logged and traced (Even, 2000). The main objective of a honeypot is focused on information gathering. Placing an easy target for an attacker within the protected infrastructure allows forensic analysts to record the intruder's activities and understand the attacker's methodology, tools and skillset. The collected forensic artifacts then create new IOCs for use in identifying other compromised systems within the organization. The collected logs and evidence can be provided to law enforcement officials during investigations and potentially lead to the prosecution of the attacker.

Author Name, email@address

Organizations deploy honeypots to simulate a server with specific vulnerable services and occasionally bait data. A honeypot's primary strength relies on its lack of business function and placement within the network. Due to the system's lack of business use, it has no active communication with users or systems without the administrator's knowledge. Security architects deploy heavy monitoring around the honeypot, including firewall logs, remote logging and network traffic sniffers. Open source and commercial honeypots exist, including Deception Toolkit, HoneyD, Modern Honey Network and Honeynet, offering many high and low-interaction honeypot tools.

Low-interaction honeypots only simulate a few features within the operating system, such as Telnet or Ssh. High-interaction honeypots provide complete operating systems with all the expected services and functions. Unfortunately, low-interaction honeypots provide a limited forensic trail, as the attacker is limited to using the services that the given honeypot makes available. Conversely, high-interaction honeypots provide extensive forensic artifacts as the attacker can migrate to services and exploit and elevate their access to the system. One drawback to high-interaction systems is that they could become a threat that provides attackers with an entry point and persistent access to the network infrastructure if not managed correctly (Jasek, 2015).

Honey agents is a term used to describe a new concept through which attackers are more quickly lured to the honeypots, accelerating the detection cycle. Honey agents could be shares, a monitored file or folder distributed across the organization. Normal users generally would not access a share file or folder or a file in a temporary folder directly. However, an APT attacker is interested in lateral movement and in identifying high-value data found in network shares and temporary files. The Honey agent directs the attacker's activities to the heavily monitored honeypot to accelerate the likelihood of detection and containment (Jasek, 2015).

2.3. Data Forensics

Tracking sensitive data at rest and in transit is vital to identifying attackers. PCI DSS and ISO 27001/27002 require control of data at rest and in transit (Payment and Security Experts, Juniper, 2015). Regardless of the type of protected data, organizations should have visibility into the locations and access associated with any protected data.

DLP provides forensic visibility into the distribution of confidential data within the infrastructure as well as access rights associated with that data.

Once an attacker compromises their target, they move the data to other systems on or off the current network. Both activities can be tracked using the DLP solutions, creating a forensic trail of data movement both at rest and in transit (Forensics and DLP Working Group, 2011). DLP can provide visibility into the location of secure data, access rights, access violations, and data movement violations along with logging and alerting. Policies can be configured to send real-time alerts when data access and movement rules are violated, providing concurrent and postmortem forensic auditing capabilities (whiteboxsecurity.com, 2015).

3. Recommendations

Forensic network design applies the same principles recommended through defense in depth. Segmentation of secure data enclaves is foundational to use appropriate forensic monitoring. Containing data, communication, users, and infrastructure within separate enclaves creates a controlled data entry and exit points. Controlled access creates a focal point allowing the application of security rules and controlling traffic flows. The flows from each enclave moving through choke points can be directed through an Intrusion and Detection system for an active response. In additional to blocking or alerting the data flows is used for logging, analysis, file extraction and matching. The volume of traffic traversing the aggregation points could require the distribution of multiple sensors across the network. Alternatively, aggregation and load balancing devices could be used to collect or distribute a large volume of traffic across multiple sensors. Several vendors offer distributed sensor architecture to provide enterprise-wide detection and logging capabilities requiring high volume inspection.

The remaining forensic monitoring infrastructure relies on passively analyzing data. Routers located at data aggregation points should be configured to export flow record data to Netflow collectors and behavior monitoring infrastructure such as Lancope's StealthWatch. The passive nature of the forensic analytics allows the use of network aggregation devices. The use of these is to collect data from multiple entry and

access points and utilize each sensor in a more efficiently. The aggregation taps could also distribute the network traffic to Pcap file analysis, extraction and matching systems. Security and routing infrastructure should export access list events and logs to behavior collection and monitoring systems. DNS records could be extracted from the network tap aggregation flows and provided to the designated monitoring solution.

Host-based intrusion prevention and DLP solutions should be deployed enterprise-wide. Each workstation, server or data warehouse is a target that should be monitored for malicious activity and presence of protected data. DLP systems also have a network component that can utilize the distributed network aggregation architecture previously discussed. In addition to host and data monitoring, honeypots and Honey agents should be deployed near protected systems. Individual honeypot server should be deployed near the servers hosting protected information. Honey agents should be deployed to at-risk systems or network shares.

Enterprise-wide forensic monitoring provides a vast amount of data. Automated behavior and baseline analysis should be deployed to reduce the volume of events requiring human review. Active forensic response requires access to all data sources and events taking place throughout the entire organization. Daily business operations are usually limited in scope as employees and customers typically perform a limited number of tasks concurrently. Attackers rely on automated tools that probes, scans and communicates with large number of systems concurrently. Having visibility across all systems while excluding known behavior provides powerful intelligence to forensic investigators. Organizations should seek the lowest possible number of aggregation consoles to review the state and events across the entire enterprise. Behavior analytics should be deployed to remove the daily standard operational events from the console allowing the analyst to focus on anomalies and exceptions.

4. Conclusion

The complexity of attacks on organizations' servers and computer/Internet infrastructures is increasing. At the same time, the amount and size of data being transmitted by organizations is growing at an exponential rate while users seek data-

access mobility. The defensive forensic network architecture is critical to providing insight into how data is accessed and used across the enterprise. Relying on a single security solution or design is no longer sufficient to protect confidential data. To apply an in-depth defense to potential security breaches, it is recommended that a multitier defense be used across the infrastructure. Intrusion detection and prevention systems offer significant forensic intelligence into malicious activities as well as into file movement. In addition to providing logging and alerting of malicious signature matching, IPS/IDS systems can be configured to extract files of interest, determine whether they are malicious, and protect other files if the malicious files pass through an enclave monitored by the security system.

Network traffic flows provide forensic logging of all network data communications through the identification of network conversations, protocols and data volume. NetFlow combined with behavior monitoring is the foundation for baseline monitoring. Organizations can use network communication logs to identify anomalies that exceed normal operation baselines. Logging is not limited to network traffic; infrastructure equipment such as firewalls, servers, DNS and applications generate Syslog events that can be exported to a remote server and correlated into a forensic event timeline. DNS, IP reputation, DLP, and honeypots can all provide IOCs and alert security analysts to anomalies or abnormal communications within their infrastructure. Designing forensic layers using multiple tiers and technologies allows forensic evaluation of events in real-time and gives organizations the opportunity to identify the appropriate response to potential data breaches. Understanding normal operation baselines and having access to historical communications and data are key to identifying and combating APT as it continues to evolve.

Author Name, email@address

5. References

cisco.com. (2015, 03 21). *Identifying Incidents via syslog*. Retrieved from cisco.com: http://www.cisco.com/web/about/security/intelligence/identify-incidents-via-syslog.html

Even, L. R. (2000, 07 12). *Intrusion Detection FAQ: What is a Honeypot?* Retrieved from sans.org: http://www.sans.org/security-resources/idfaq/honeypot3.php

Forensics and DLP Working Group. (2011, 06 01). *Digital Forensics and Data Leakage protection best practices*. Retrieved from intelisecure.com: https://www.intelisecure.com/wp/wp-content/uploads/2013/06/pdf_30.pdf

Garbrecht, F. C. (2015, 04 25). *Practical Implementation of Syslog in Mixed Windows Environment for Secure Centralized Audit Logging.* Retrieved from SANS.org: http://www.sans.org/reading-room/whitepapers/casestudies/practical-implementation-syslog-mixed-windows-environments-secure-centralized-audit-loggi-713

GTKKlondike. (2015, 03 23). *Open Source Network Forensics and Advanced Pcap Analysis*. Retrieved from slideshare.net: http://www.slideshare.net/GTKlondike/open-source-network-forensics-and-advanced-pcap-analysis

Hipolito, J. M. (2014, 12 13). *Anatomy of a Data Breach*. Retrieved from Trendmicro.com: http://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/110/anatomy-of-a-data-breach

infoblox.com. (2015, 03 29). *Improved Security Through DNS Inspection*. Retrieved from Infoblox.com: https://community.infoblox.com/blogs/2014/02/18/improved-security-through-dns-inspection-part-2

ISACA. (2013). *Advanced Persistent Threats: How to Manage the Risk to your Business.* ISACA.

Author Name, email@address

lancope.com. (2015, 03 22). *The Role of NetFlow in Digital Forensics and Incident Response*. Retrieved from Lancope.com: http://www.lancope.com/blog/netflow-forensics-incident-response

Lang, J.-P. (2015, 03 15). *openinfosecfoundation.org*. Retrieved from Suricata Rules: File-Keywords: https://redmine.openinfosecfoundation.org/projects/suricata/wiki/File-keywords

Liu, D. (2009). *Cisco Router and Switch Forensics: Investigating Malicious Network Activies.* Rockland, MA: Syngress.

Mcafee.com. (2015, 03 07). *Diary of a "RAT" (Remote Access Tool)*. Retrieved from mcafee.com: https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/23000/PD23258/en_US/Diary_of_a_RAT_datasheet.pdf

nist.gov. (2015, 04 25). *Guide to Integrating Forensic Techniques into Incident Response*. Retrieved from National Institute of Standards and Technology: http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf

openinfosecfoundation.org. (2015, 03 29). *IP Reputation Config*. Retrieved from openinfosecfoundation.org: https://redmine.openinfosecfoundation.org/projects/suricata/wiki/IPReputationConfig

openinfosecfoundation.org. (2015, 03 15). *openinfosecfoundation.org*. Retrieved from openinfosecfoundation.org: https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Suricata_yaml

openinfosecfoundation.org. (2015, 03 15). *Suricata: File Extraction*. Retrieved from openinfosecfoundation.org: https://redmine.openinfosecfoundation.org/projects/suricata/wiki/File_Extraction

opswat.com. (2015, 03 15). *MetaScan Package Options*. Retrieved from opswat.com: https://www.opswat.com/products/metascan/packages

Author Name, email@address

Payment and Security Experts, Juniper. (2015, 04 25). *Implementing PCI, A Guide for Network Security Engineers*. Retrieved from juniper.com: http://www.juniper.net/us/en/local/pdf/whitepapers/2000268-en.pdf

Randall, L. (2013, 02 27). *Bro IDS How To: File Extraction using HTTP, FTP, SMTP, and IRC*. Retrieved from Applied Network Security Monitoring: http://www.appliednsm.com/bro-ids-2-1-file-extraction-how-to/

ROMAN JASEK, M. K. (2015, 04 04). *APT Detection system using honeypots*. Retrieved from Tomas Bata University: http://www.wseas.us/e-library/conferences/2013/Valencia/ACIC/ACIC-02.pdf

splunk.com. (2015, 03 21). *Operational Intelligence*. Retrieved from Splunk.com: http://www.splunk.com/en_us/resources/operational-intelligence.html

Suricata-ids.org. (2015, 03 09). *All Features, Complete list of Suricata Features*. Retrieved from Suricata: http://suricata-ids.org/features/all-features/

TrendMicro. (2012). *Spear-Phishing Email: Most Favored APT Attack Bait*. Retrieved from TrendMicro.com: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf

TrendMicro Global R&D Center. (2015, 03 07). *Data Exfilteration: How DO Threat Actors Steal Your Data?* Retrieved from trendmicro.com: http://about-threats.trendmicro.com/cloud-content/us/ent-primers/pdf/how_do_threat_actors_steal_your_data.pdf

whiteboxsecurity.com. (2015, 04 04). *Real-Time Forensics & Active Discovery*. Retrieved from whiteboxsecurity.com: http://www.whiteboxsecurity.com/product-tour/whiteops/

Author Name, email@address

Last Updated: July 16th, 2018

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Riyadh July 2018	Riyadh, SA	Jul 28, 2018 - Aug 02, 2018	Live Event
SANS Pittsburgh 2018	Pittsburgh, PAUS	Jul 30, 2018 - Aug 04, 2018	Live Event
Security Operations Summit & Training 2018	New Orleans, LAUS	Jul 30, 2018 - Aug 06, 2018	Live Event
SANS Hyderabad 2018	Hyderabad, IN	Aug 06, 2018 - Aug 11, 2018	Live Event
Security Awareness Summit & Training 2018	Charleston, SCUS	Aug 06, 2018 - Aug 15, 2018	Live Event
SANS Boston Summer 2018	Boston, MAUS	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS San Antonio 2018	San Antonio, TXUS	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS August Sydney 2018	Sydney, AU	Aug 06, 2018 - Aug 25, 2018	Live Event
SANS New York City Summer 2018	New York City, NYUS	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS Northern Virginia- Alexandria 2018	Alexandria, VAUS	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS Krakow 2018	Krakow, PL	Aug 20, 2018 - Aug 25, 2018	Live Event
Data Breach Summit & Training 2018	New York City, NYUS	Aug 20, 2018 - Aug 27, 2018	Live Event
SANS Chicago 2018	Chicago, ILUS	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Prague 2018	Prague, CZ	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Virginia Beach 2018	Virginia Beach, VAUS	Aug 20, 2018 - Aug 31, 2018	Live Event
SANS San Francisco Summer 2018	San Francisco, CAUS	Aug 26, 2018 - Aug 31, 2018	Live Event
SANS Copenhagen August 2018	Copenhagen, DK	Aug 27, 2018 - Sep 01, 2018	Live Event
SANS SEC504 @ Bangalore 2018	Bangalore, IN	Aug 27, 2018 - Sep 01, 2018	Live Event
SANS Wellington 2018	Wellington, NZ	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Amsterdam September 2018	Amsterdam, NL	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Tokyo Autumn 2018	Tokyo, JP	Sep 03, 2018 - Sep 15, 2018	Live Event
SANS Tampa-Clearwater 2018	Tampa, FLUS	Sep 04, 2018 - Sep 09, 2018	Live Event
SANS MGT516 Beta One 2018	Arlington, VAUS	Sep 04, 2018 - Sep 08, 2018	Live Event
Threat Hunting & Incident Response Summit & Training 2018	New Orleans, LAUS	Sep 06, 2018 - Sep 13, 2018	Live Event
SANS Baltimore Fall 2018	Baltimore, MDUS	Sep 08, 2018 - Sep 15, 2018	Live Event
SANS Alaska Summit & Training 2018	Anchorage, AKUS	Sep 10, 2018 - Sep 15, 2018	Live Event
SANS Munich September 2018	Munich, DE	Sep 16, 2018 - Sep 22, 2018	Live Event
SANS London September 2018	London, GB	Sep 17, 2018 - Sep 22, 2018	Live Event
SANS Network Security 2018	Las Vegas, NVUS	Sep 23, 2018 - Sep 30, 2018	Live Event
SANS DFIR Prague Summit & Training 2018	Prague, CZ	Oct 01, 2018 - Oct 07, 2018	Live Event
Oil & Gas Cybersecurity Summit & Training 2018	Houston, TXUS	Oct 01, 2018 - Oct 06, 2018	Live Event
SANS Brussels October 2018	Brussels, BE	Oct 08, 2018 - Oct 13, 2018	Live Event
SANS Pen Test Berlin 2018	OnlineDE	Jul 23, 2018 - Jul 28, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced