Analista forense em um Centro de Operações de Segurança - Análise de pacotes de um ataque malware

Pedro Fernando Moreira Silva Antunes
Departamento de Ciências de Computadores
Faculdade de Ciências da Universidade do Porto
Porto, Portugal
up201507254@fc.up.pt

André Ferreira Monteiro Lopes Rodrigues
Departamento de Ciências de Computadores
Faculdade de Ciências da Universidade do Porto
Porto, Portugal
up201505639@fc.up.pt

***Abstract*—Este projeto tem como objetivo a exploração do trabalho de um analista forense em um centro de operações de segurança para perceber como é que os ataques informáticos são investigados, mais concretamente a investigação e análise de pacotes. Numa primeira fase, abordam-se os componentes utilizados de um SOC e algumas ferramentas de análises de pacotes como o Wireshark e tcpdump. Seguindo-se da implementação e a solução de um ataque exemplo de malware. Por fim, apresentamos os resultados obtidos na investigação deste ataque e introduzimos algumas recomendações para o trabalho de um analista forense.**

I. Introdução

O nosso objectivo com este trabalho foi perceber de que forma é que um centro de operações de segurança pode resolver investigações forenses de ataques informáticos com uma procura de evidências digitais.

Para isso iremos simular um ataque de malware, onde depois iremos focar-nos na análise dos pacotes que circularam pela rede com o intuito de encontrar evidências do ataque. Os pacotes foram capturados e guardados num ficheiro PCAP. Depois será feito uso de uma SIEM, onde encaminharemos o PCAP para um IDS para que sejam gerados alertas, que depois sejam processamos e dêem entrada na pilha ELK (ElasticSearch, Logstash e Kibana). Ao longo da investigação, iremos mostrar ferramentas que complementam a SIEM. Posto isto, através de uma inspecção profunda dos pacotes, investigamos as evidências do ataque para prevenirmos ataques semelhantes e identificarmos os autores do ataque.

II. Estado de arte

Um SOC (Security Operations Center) tem um papel fundamental quando nos referimos à segurança informática. Através de equipas organizadas e divididas por níveis, fornece uma defesa contra actividades maliciosas sobre uma rede computacional, assim como sobre os recursos humanos que actuam no sistema. Identificação, prevenção, protecção, detecção, resiliência, resposta, redacção e recuperação são as únicas palavras do dicionário de um SOC. Apesar de serem poucas palavras, cada uma exige imenso trabalho para nos garantir a segurança do sistema. Mesmo com a máxima segurança imaginável implementada por um SOC, temos de ter consciência que naturalmente chegará o dia em que o nosso SOC irá falhar em algum aspecto e que estaremos a ser alvos de um ataque. Como foi dito, o SOC é composto por equipas organizadas. Quando há um ataque, também há uma equipa preparada para efectuar a análise forense do ataque. As investigações forenses têm como objectivo identificar o autor do ataque e analisar a informação proveniente de outras equipas que actuam no SOC para conseguir reconstruir o ataque. Um analista forense tem de conseguir prevenir futuros ataques iguais ao ataque sucedido.

Posto isto, apresentamos algumas ferramentas e componentes do SOC necessários para a análise forense.

A. IDS/IPS - Suricata [4]

Um IDS (Intrusion Detection System) é um componente de um SOC e monitoriza o sistema sem alterar os pacotes de rede, na procura de falhas que possam indicar uma invasão à rede. Um IPS (Intrusion Prevention System) completa as funções do IDS com o controlo de intrusos. Caso encontre algum intruso na rede, o IPS impede que o pacote seja entregue. Reprograma a firewall e bloqueia o endereço IP do intruso prevenindo problemas maiores.

- ***Suricata:***
  O suricata é um IDS/IPS open-source e funciona com assinaturas, ou regras, para detectar anomalias no tráfego da rede. Essas regras são formas de análise de pacotes (por exemplo através de diferentes protocolos) e de reconhecimento de palavras (permite também fazer scripting), que quando acertam um determinado critério despoletam um alerta/evento. Como era espectável podemos fazer as nossas próprias regras bem como usar as regras padrão fornecidas pelo suricata, que já fazem um bom trabalho, contudo são generalistas. O suricata foi instalado através de um docker e foi utilizado transformar o PCAP em alertas/eventos definidos pelas regras num ficheiro JSON.

B. SIEM - ”ELK Stack”

O IDS faz parte de uma SIEM (Security Information and Event Management), que é uma estrutura lógica composta por várias ferramentas que proporcionam a análise de alertas/eventos gerados a partir de actividades da rede ou do sistema operativo dos dispositivos que estão a ser monitorizados. Portanto, a SIEM está num dispositivo único e é responsável por monitorizar a actividade dos dispositivos na rede bem como da própria rede proporcionado em tempo real uma análise de ambos, bem como mantém registos dessa actividades para que possamos usar em situações como a deste artigo. Iremos falar de algumas destas ferramentas em mais detalhe mais a frente.

A SIEM é também constituída por ferramentas que permitem armazenar dados, como uma base de dados, onde depois é possível fazer pesquisas, analisar e até visualizar os dados em tempo real. Neste caso a SIEM está a correr a “ELK Stack” que é um conjunto de três ferramentas open source desenvolvidas pela empresa “elastic” e o seu acrónimo traduz-se em Elastic, Logstash e Kibana que são as ferramentas que nos fornecem as funcionalidades citadas anteriormente e que nós iremos aprofundar a seguir. A ”ELK Stack” foi instalada através de um docker.

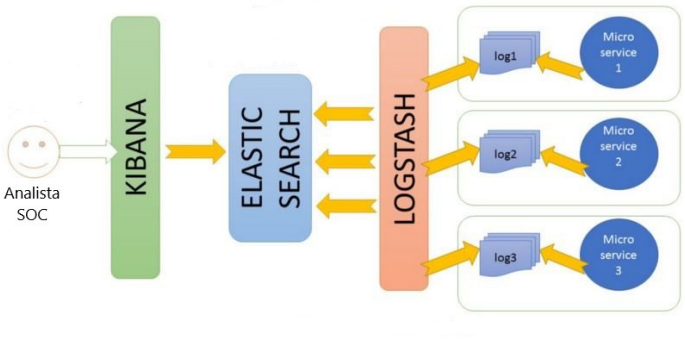

Fig. 1. Interação da ”ELK Stack” com diferentes aplicações a gerar ficheiros de log

- ***Filebeat: [5]***
  O Filebeat é um agente leve para encaminhar e centralizar dados de logs. O Filebeat fica à escuta de ficheiros num diretório ou num servidor. Enquanto faz a monitoria no local específicado dos ficheiros de log, caso receba uma entrada nova (um beat) envia os logs para o Logstash onde irão estar sujeitos a uma indexação. O Filebeat também pode encaminhar os beats diretamente para o Elasticsearch.
  No nosso caso, o Filebeat foi configurado para estar sempre à escuta de novos ficheiros JSON provenientes do Suricata. É de realçar que este processo de escuta de logs gerados pelo Suricata poderia ter sido implementado através do Logstash. No entanto, teríamos de configurar manualmente o Logstash para cada caso. Colocando o Filebeat como um nó intermédio neste processo, estamos sempre à escuta de novos beats.

- ***Logstash: [6]***
  O Logstash é uma ferramenta para recolher, processar e encaminhar eventos e mensagens de log. A recolha é realizada através plug-ins configuráveis de entrada que neste caso os ficheiros de entrada são recebidos pelo Filebeat. Depois da configuração de entrada, os logs podem ser processados por filtros que transformam e normalizam os dados do evento. Na nossa implementação, utilizamos os filtros de JSON na normalização dos logs.
  Por fim, o Logstash reencaminha os eventos para plug-ins de saída. Estes podem encaminhar os eventos para uma variedade de programas externos, incluindo o Elasticsearch que foi o nosso caso.

- ***Elasticsearch: [7]***
  O Elasticsearch é o elemento central da pilha ELK e trabalha sobre índices de dados. Pode receber estes índices de diversas fontes, incluindo do Logstash que foi o nosso caso. Durante o processo de indexação, o Elasticsearch armazena os índices como documentos JSON e utiliza uma estrutura de dados de índices invertidos que permite pesquisas de dados complexas com tempos de pesquisa extremamente rápidos. As pesquisas do Elasticsearch podem ser visualizadas no Kibana através de um browser.

- ***Kibana: [8]***
  O Kibana é o elemento final da pilha ELK e é onde podemos ter uma visão final de tudo o que foi feito. O Kibana permite a visualização e gestão dos índices inseridos no Elasticsearch e fornece um vasto leque de gráficos e painéis em tempo real de monitoria dos dados.

C. Analisadores de pacotes [3]

Embora a pilha ELK e o suricata nos fornecem informações sobre os pacotes armazenados, por vezes estas informações não são suficientes para que a análise forense seja bem sucedida. Quando é necessário realizar uma análise profunda dos pacotes, como analisar os estados de sessões TCP, temos de recorrer a outras ferramentas de análises de pacotes. Neste trabalho acabamos por utilizar ferramentas para análises de PCAP (conjunto de pacotes de rede):

- ***Wireshark***
  Ferramenta com interface gráfica, com hipótese de utilização de filtros. Excelente escolha para PCAPs pequenos.
- ***Tcpdump***
  Ferramenta de linha de comandos sem interface gráfica, o que nos permite capturar e analisar pacotes através de um acesso remoto.

III. Implementação [1]

Foi nos entregue um ficheiro PCAP, que é um ficheiro com capturas de pacotes, e é um recurso fundamental em qualquer investigação forense, pois permite nos reconstruir o tráfego

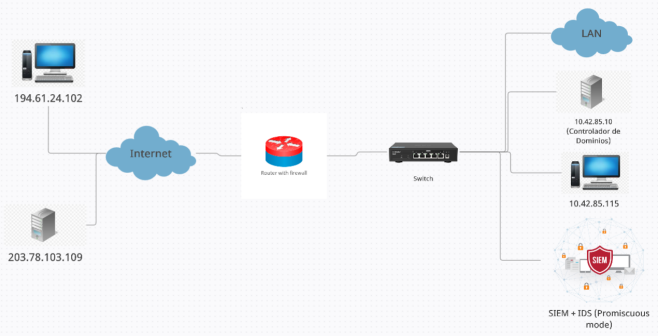

Fig. 2. Constituency

de da(s) rede(s). Os PCAP são formados por pacotes que são capturados através de sensores. Normalmente existem vários sensores espalhados pela rede no qual são encaminhados e posicionados através de um IDS/IPS, no caso o suricata, como já foi referido. Para obter mais informação acerca do PCAP iremos correr o comando ”capinfos” sobre o nosso ficheiro PCAP. Através deste comando vemos que número de pacotes que constituem o PCAP é elevadíssimo (quase meio milhão de pacotes) e portanto o primeiro passo que um analista forense deve tomar é separar o essencial do não essencial e para tal iremos usar as ferramentas da SIEM. Como já foi referido, o suricata utiliza um conjunto de regras para gerar alertas, então o próximo passo lógico será usar o suricata para converter aquele número grande de pacotes num número muito mais pequeno de alertas, alertas esses que esperamos que nos sirvam para detectar anomalias no tráfego da rede posteriores ao ataque. Para gerar o ficheiro com os alertas executamos o comando “suricata -r case001.pcap”, onde o suricata irá correr em modo replay, gerando um ficheiro log com os alertas. Executando o comando ”wc” (word count) sobre o ficheiro com os alertas podemos ver que foram gerados 256 alertas, contra quase meio milhão de pacotes do PCAP.

Agora a próxima etapa consiste em analisar os 256 alertas, montando assim a nossa investigação. Como dito no estado da arte, o suricata está pré-configurado na SIEM para enviar os seus logs para serem armazenados e visualizados através da ”ELK Stack”, portanto iremos visualizar os alertas através da interface web proporcionada pelo kibana. No kibana podemos analisar os 256 alertas, no qual cada alerta está dividido pelos campos: timestamp; protocolo; detalhes específicos para cada protocolo; classificação do alerta; prioridade; protocolo de transporte usado; endereço IP do emissor e endereço IP do receptor. Ao analisar os alertas devemos estar atentos a certas referências sobre a ”kill chain”, por isso um analista forense deve ter conhecimento sobre exploits e ”red team” para que possa ser capaz na parte da defesa desses exploits. Felizmente para nós, com os alertas foi possível detectar pacotes que utilizavam o protocolo ICMP e no qual o suricata conseguiu detectar que eram provenientes do programa NMAP que faz uso de pacotes ICMP Ping. Ao olhar para o alerta percebemos que alguém com o endereço IP 192.61.24.102 tentou descobrir mais informação acerca do endereço privado 10.42.85.10 que é um controlador de domínios. Ao visualizar os alertas subsequentes observamos que o atacante tentou fazer vários pedidos a esse serviço, e qual metodologia de ataque consiste em fazer um elevado número de pedidos num curto período de tempo? um ataque de força bruta! Vamos usar esse endereço IP como nosso ponto de pivot, que é um ponto de importância encontrado ao analisar a informação e que nos permite ter um senso maior do acontecido de forma mais rápida e eficaz.

Agora que temos um ponto de pivot, vamos utilizar outras ferramentas para vasculhar o PCAP de forma mais rápida, de forma a encontrar mais informação relevante. Infelizmente, por agora teremos de abandonar o suricata e SIEM, pois como vimos muitos pacotes não geraram alertas, mas no entanto ainda podem ser importantes na investigação pois podem ainda conter informação sobre o estado da rede antes do sucedido e porque as regras pelo seu formato generalista, derivado a dependerem do que é a ação normal dos utilizadores da rede e também por dependerem de conhecimento prévio acerca de ”kill chains” de ataques, podem fazer com que certos pacotes importantes não gerem alertas (falsos negativos). Contudo os alertas desempenham um papel essencial, no qual na maioria dos casos nos fornece um ponto de partida para acharmos os nossos pontos de pivot. A partir deste momento iremos utilizar a ferramenta ”tcpdump” que nos permite analisar pacotes (um pcap é uma colecção de pacotes). Iremos visualizar apenas os pacotes que tenham o endereço de receptor igual a 194.61.24.102 (o nosso ponto de pivot), o que nos permitirá obter os pacotes ICMP Echo usados pelo NMAP, bem como os pacotes que o controlador de domínios envia como resposta. Aqui ao contrário do que podia ser visto no kibana, temos acesso às flags TCP enviadas nos pacotes, enquanto que o suricata apenas indicava o tipo de protocolo usado no transporte. Com o tcpdump é possível observar que o atacante ao mesmo tempo que envia o pacote ICMP Echo, também envia um SYN para a porta 443 e um ACK para a porta 80, isto demonstra que foi utilizado de facto o NMAP, tanto o SYN scan, como o ACK scan, entre outros. O facto curioso é que o scan foi direccionado para a porta 3389 do nosso controlador de domínios (10.42.85.10) sem antes ter ocorrido nenhum scan e isto deve-se ao facto do controlador estar aberto para a Internet, o que faz com que seja detectado e indexado pelos motores de buscas. Este serviço não deveria de forma alguma estar exposto para a Internet, caso fosse necessário aceder de forma remota a este serviço, os utilizadores deveriam usar VPNs. Outra coisa é que com os alertas do suricata podíamos observar troca de pacotes RDP (Remote Desktop Protocol) entre 194.61.24.102 e 10.42.85.10, mas contudo não havia nenhum alerta para pacotes RDP entre hosts internos. Será que conseguimos visualizar se houve troca de pacotes RDP entre hosts da rede da organização?

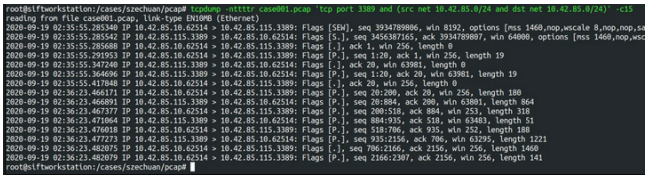

Fig. 3. Troca de pacotes RDP entres hosts internos

Como podemos observar pela imagem, houve sim troca de pacotes entre o endereço 10.42.85.10 (controlador de domínios) e o endereço 10.42.85.115 (desktop), esta informação será nos útil para compreender melhor o próximo passo. Posto isto, o ideal agora é utilizar o tcpdump para fazer o ”dump” de todos os pacotes onde o endereço IP 194.61.24.102 está envolvido, desta forma obtendo um PCAP de tamanho menor, onde passaremos a utilizar a ferramenta ”Wireshark”, pois é uma ferramenta que se torna viável quando se têm um PCAP de pequeno tamanho. Com o wireshark iremos fazer o mesmo que temos vindo a fazer, que é analisar os pacotes, contudo o wireshark possui várias ferramentas úteis neste processo, uma delas é o menu que nos possibilita ver os ”endpoints”. E é aqui que ficamos a saber que o tal 10.42.85.115 comunicou com o IP do nosso suspeito (194.61.24.102). Agora o nosso ponto de pivot tornou-se o 10.42.85.115 e portanto iremos procurar no wireshark por esse endereço IP, onde nos será mostrado trocas de pacotes TCP e HTTP. Num dos pacotes HTTP percebemos que o utilizar da rede local acedeu a um IP onde fez download de um ficheiro .exe suspeito.

Fig. 4. Pacote HTTP - download do malware

De forma resumida, depois de fazer o download do ficheiro, comparar a sua hash com uma base de dados de malware, analisar o ficheiro de forma mais aprofundada e correr o ficheiro num ambiente ”sandbox” percebemos que se trata de um malware que comunica com o servidor 203.78.103.109. Ao analisar novamente o PCAP com o wireshark percebemos que o 10.42.85.115 trocou pacotes com o endereço IP 203.78.103.109.

IV. Resultados

Nós começamos por utilizar um IDS, o suricata, que estava configurado na SIEM da organização, para correr um ficheiro PCAP. Ao fazer isso, o suricata originou um conjunto de alertas que depois enviou para Elasticsearch, para que pudéssemos analisar através do Kibana. Depois de fazer a análise dos alertas, percebemos que o endereço IP 194.61.24.102 (nosso suspeito) realizou um NMAP, seguido de um ataque de força bruta ao controlador de domínios (10.42.85.10). Com base no endereços IP da vitima analisamos os pacotes do PCAP em mais detalhe para percebermos outra actividade com base nesse endereço IP, e reduzimos essa informação a um novo PCAP mais pequeno. Ao analisar esse novo PCAP percebemos que provavelmente o controlador de domínios e a maquina 10.42.85.115 estavam comprometidos, descobrindo um ficheiro .exe, no qual ambas as máquinas fizeram download. Depois foi corrido esse ficheiro em modo sandbox, no qual conseguimos perceber que o malware comunicava com o endereço IP 203.78.103.109. Ou seja, o atacante conseguiu fazer realizar o ataque de força bruta ao controlador de domínios e depois conseguiu aceder ao desktop (10.42.85.115) realizando o download do malware. Foi possível detectar que o malware funcionou pois vimos tráfego entre 10.42.85.115 e 203.78.103.109.

V. Conclusões

Começamos este artigo por identificar a ”constituency” da organização, bem como partes chaves da SOC, como a SIEM, que fornece ferramentas importantes para que um analista forense possa montar a sua investigação. Vimos de forma geral como a SIEM é composta e como as diversas ferramentas se interligam. Como dito anteriormente, a SIEM proporciona formas de encontrar os pontos de pivot, extraindo apenas a informação essencial com os alertas, permitindo manipular e gerar os nossos próprios alertas, bem como manipular a informação que pretendemos extrair dos alertas/logs para depois ser analisada no kibana, este processo permitem depois acelerar a investigação. Contudo as ferramentas da SIEM não permitem cobrir toda a investigação, pois como vimos estão dependentes de regras que focam-se em ataques conhecidos ou no conceito de normalidade da redes e dos dispositivos, ou seja, um atacante experiente pode tentar camuflar o seu ataque ou operar dentro da normalidade aceite pela SIEM. Portanto depois é essencial olhar para o resto dos pacotes que não geraram alertas, com base nos pontos de pivot (pontos de importância), neste caso usamos a ferramenta tcpdump. E dessa forma retirar novas ilações e voltar a reduzir o PCAP num outro muito pequeno, em comparação, que depois será analisado por outra ferramenta especifica para isso, o wireshark. Convém resalvar que este PCAP mais pequeno é muito diferente dos alertas gerados pelo suricata, pois já utiliza mais pontos de pivot e outro conjunto de pacotes que não geraram alertas, mas que são importantes na investigação. O trabalho de um analista forense consiste em analisar a informação, extrair ilações e com base nisso extrair apenas o essencial, reduzindo a cada passo a investigação até chegar às conclusões finais.

REFERENCES

[1] Case 001 PCAP Analysis, URL https://dfirmadness.com/case-001-pcap-analysis/

[2] Leslie F. Sikos, Packet analysis for network forensics: A comprehensive survey, Forensic Science International: Digital Investigation, Volume 32, 2020, 200892, ISSN 2666-2817

[3] F. Hock and P. Kortiš, "Commercial and open-source based Intrusion Detection System and Intrusion Prevention System (IDS/IPS) design for an IP networks," 2015 13th International Conference on Emerging eLearning Technologies and Applications (ICETA), Stary Smokovec, 2015, pp. 1-4, doi: 10.1109/ICETA.2015.7558466.

[4] IDS/IPS - Suricata, URL https://suricata-ids.org/

[5] Elastic - Filebeat, URL https://www.elastic.co/pt/beats/filebeat

[6] Elastic - Logstash, URL https://www.elastic.co/pt/logstash

[7] Elastic - Elasticsearch, URL https://www.elastic.co/pt/what-is/elasticsearch

[8] Elastic - Kibana, URL https://www.elastic.co/pt/kibana