

Coleta de Artefatos Maliciosos na Internet Brasileira

Pedro Henrique Matheus da Costa Ferreira, Antonio Montes Filho, Ferruccio de Franco Rosa e Walcir Marcelino Cardoso Júnior

Centro de Tecnologia da Informação Renato Archer Rodovia Dom Pedro I (SP - 65) Km 143,6 Bairro: Amaraes Campinas - São Paulo Brasil CEP: 13069-901

Resumo — Nesse artigo apresenta-se uma proposta de abordagem para capturar e armazenar artefatos maliciosos de software. A abordagem possibilita a substituição dos sensores e do túnel criptografado por *Honeypots* e a comunicação direta do *Honeypot* com um coletor centralizado utilizando criptografia. É possível o envio das informações de um único artefato malicioso de software para o coletor centralizado, mesmo proveniente de instituições diferentes, e a criação de grupos e domínios para que cada instituição acesse apenas os artefatos coletados pelos seus *Honeypots*. Como resultados verificados, podem-se citar a redução de até 70% na utilização do link de comunicação, o aumento da segurança, pois houve um isolamento dos artefatos maliciosos de software em cada instituição, além do aumento dos registros de ataques.

Palavras-Chave — Detecção de Intrusão, Malware, *Honeypots*.

I. INTRODUÇÃO

Nos dias atuais existe uma preocupação muito grande com a propagação e disseminação de artefatos maliciosos que podem comprometer a segurança das informações e das redes como um todo, partindo desde um simples usuário até grandes corporações civis e militares.

No mundo todo é comum o uso de ferramentas para monitorar as atividades de artefatos maliciosos, com o intuito de proteger os sistemas e as redes de ataques. Isso é particularmente importante em sistemas críticos nos quais, além de se saber que houve um ataque, é importante se saber de onde partiu, qual era o objetivo e quem estava por trás do ataque.

Por esse motivo vem-se coletando, armazenando e analisando artefatos maliciosos, de modo que seja possível identificar alguns vetores como a origem, o objetivo do artefato e tipo de propagação (Vulnerabilidades de sistemas, Sites Maliciosos, SPAM, Rede, etc.)

II. OBJETIVOS

Nesse trabalho apresenta-se uma abordagem para capturar e armazenar artefatos maliciosos de software, que são disseminados pela rede buscando explorar vulnerabilidades nos sistemas. Para simular essas vulnerabilidades, utiliza-se *Honeypots* de baixa interatividade e um sistema distribuído de detecção de intrusões conhecido como SURFids [1].

Segundo Provos [2], *Honeypots* de baixa interatividade, emulam serviços, pilhas de rede, ou outros aspectos de uma máquina real. Eles permitem ao atacante uma interação

limitada com o sistema alvo e que nos permitem conhecer as informações quantitativas, principalmente sobre o ataque. Por exemplo, um serviço HTTP emulado pode apenas responder para uma requisição de um arquivo particular, e necessita apenas implementar uma parte da especificação HTTP.

O nível de interação deve ser somente o necessário para enganar o atacante ou uma ferramenta automatizada como um “worm” que está procurando por um arquivo específico para comprometer o servidor. A grande vantagem dos *Honeypots* de baixa interatividade é a simplicidade e a facilidade de manutenção. Normalmente o *Honeypot* de baixa interatividade é instalado e liberado para coletar os dados, sem muitas configurações [2]. Esses dados podem ser uma cópia do artefato utilizado no ataque e também o histórico detalhado do ataque. São exemplos de *Honeypots* de baixa interatividade o Nepenthes [3] e o Dionaea [4].

Os dados coletados pelos *Honeypots* são armazenados em uma base de dados centralizada, onde podem ser analisados por uma série de ferramentas e disponibilizados por um sistema distribuído utilizado para detecção de intrusão.

III. REVISÃO DA LITERATURA

Neste tópico são apresentadas técnicas atuais para detecção de intrusão em redes.

Safaa et al. [8] apresentam uma abordagem para reduzir os falsos positivos em detectores de intrusão. Tal abordagem baseia-se na análise das causas raízes que culminam com o disparo do alarme e, a partir desta análise, agrupamentos de alarmes com características similares são montados visando modelar um formato semi-automático de análise, permitindo a um analista de segurança detectar as causas raízes destes falsos alarmes.

García-Teodoro et al. [9], apresentam um sumário das técnicas mais conhecidas de detecção de intrusão baseadas em anomalias, descrevem quais sistemas estão em desenvolvimento, que pesquisas sobre o assunto estão em andamento e quais são os principais desafios para esta linha de pesquisa. Os principais desafios apresentados pelos autores são: eliminação dos falsos positivos, a ausência de métricas apropriadas para detectores de intrusão, a análise de dados cifrados e problemas de desempenho de detectores de intrusão em redes de alta velocidade.

Zhonglin [10] introduz um modelo de detecção baseado no princípio *choose-closed* sob a perspectiva de um sistema de detecção de intrusão. Este modelo proposto processa características de intrusão utilizando lógica *fuzzy*, objetivando aumentar a qualidade de detecção. O autor afirma que conseguiu uma significativa melhora no desempenho da detecção.

IV. SURFids

O SURFids é um Sistema Distribuído de Detecção de Intrusão (D-IDS) baseado em sensores passivos, cujo objetivo é prover um alerta antecipado ao administrador da rede, sobre os sistemas que tenham sido comprometidos.

Os D-IDS contam em muitos casos, com uma abordagem cliente/servidor onde o cliente é chamado de sensor, e que atende às seguintes regras:

- O sensor deve ser executado “out-of-the-box”;
- O sensor deve ser completamente passivo e, portanto livre de manutenção;
- A D-IDS não deve gerar alertas falsos positivos;
- Um sensor deve ser capaz de ser executado em uma rede padrão;
- Deverá permitir a comparação de estatísticas geradas pelos sensores ou grupo de sensores.

Na versão padrão do SURFids uma estação de trabalho comum é transformada em sensor. O sistema operacional é inicializado a partir de um pendrive contendo o software sensor SURFnet D-IDS. Esse pendrive contém uma versão modificada do sistema operacional Knoppix [5] e usa o OpenVPN [5] para iniciar um túnel criptografado de camada 2 para o servidor D-IDS.

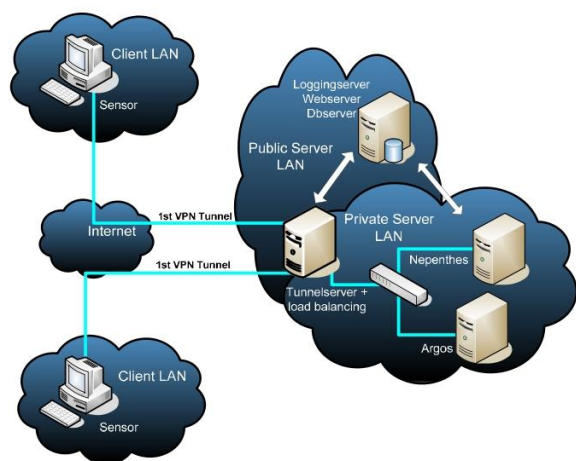


Fig. 1. Modelo de rede utilizada pelo SURFids

O túnel deve ser colocado em modo de ponte entre o sensor e o servidor D-IDS. Em seguida, um pedido de DHCP é feito a partir do servidor D-IDS através do túnel para a rede do cliente. Este pedido permite que o servidor D-IDS obtenha um endereço IP na rede do cliente que é, vinculado a uma interface virtual de um Honeypot.

Desta forma, o servidor D-IDS estará presente na rede do cliente e os atacantes vão pensar que estão atacando um equipamento da rede do cliente.

O Honeypot que está sendo usado no servidor D-IDS pode ser o Nepenthes ou o Dionaea, que são capazes de simular determinadas vulnerabilidades conhecidas.

Se ocorrer um acesso ao Honeypot isso é considerado um ataque e o Honeypot tenta capturar o artefato que o invasor utiliza para infectar o equipamento e uma vez completado o ataque, o atacante acredita ter comprometido o equipamento real.

Todos os ataques são registrados em um banco de dados PostgreSQL [7] e os usuários podem visualizar informações detalhadas sobre os ataques através de uma interface Web. Na Figura 1 pode-se visualizar como é montada uma rede SURFids.

Desta forma o SURFids atende as instituições que tem uma grande rede com vários escritórios ou filiais espalhadas por diferentes localidades, onde se trabalha com segmentos de redes diferentes e onde não se pode ter um Honeypot instalado em cada local. Mas essa abordagem apresenta algumas restrições, como por exemplo quando se pretende integrar varias instituições diferentes que tem seus próprios Honeypots ou que preferem dedicar equipamentos exclusivos para a função de sensor.

V. DELIMITAÇÃO DO PROBLEMA

A arquitetura utilizada pelo SURFids, apesar de ser muito bem construída e idealizada, apresenta restrições que podem inviabilizar o seu uso por um grupo de instituições que queiram partilhar a captura de artefatos. Vejamos algumas dessas restrições:

- Cada sensor exige a utilização de um único endereço IP válido na rede do cliente. Se há a necessidade de se utilizar vários sensores, haveria a necessidade de se ter vários endereços válidos, gerando aumento de custo;
- Se há vários endereços IP válidos disponíveis, haverá a necessidade de se instalar vários sensores, gerando maior carga de trabalho e dificuldade para administração;
- A conexão realizada entre os sensores e o servidor exige uma grande largura de banda para suportar uma grande quantidade de ataques;
- Os artefatos capturados em instituições diferentes não estariam acessíveis aos demais;
- Todo processamento dos ataques é centralizado, exigindo grande poder de processamento;
- Não permite uma rede heterogênea, contendo Dionaea e Nepenthes operando juntos, por exemplo;
- Não aproveita os Honeypots já em funcionamento, gerando a necessidade de se instalar novos sensores.

VI. ABORDAGEM PARA COLETA DE ARTEFATOS MALICIOSOS NA INTERNET BRASILEIRA

A abordagem proposta é uma adaptação do Sistema Distribuído de Detecção de Intrusão SURFids. As modificações na arquitetura do SURFids foram as seguintes:

- Substituição dos Sensores e do túnel criptografado por Honeypots;
- Comunicação direta do Honeypot com um coletor centralizado utilizando criptografia;
- Envio para o coletor centralizado de um único artefato malicioso de software, mesmo proveniente de instituições diferentes;
- Criação de grupos e domínios para que cada instituição veja apenas os artefatos coletados pelos seus Honeypots;

A Figura 2 mostra como é organizada a rede após as modificações.

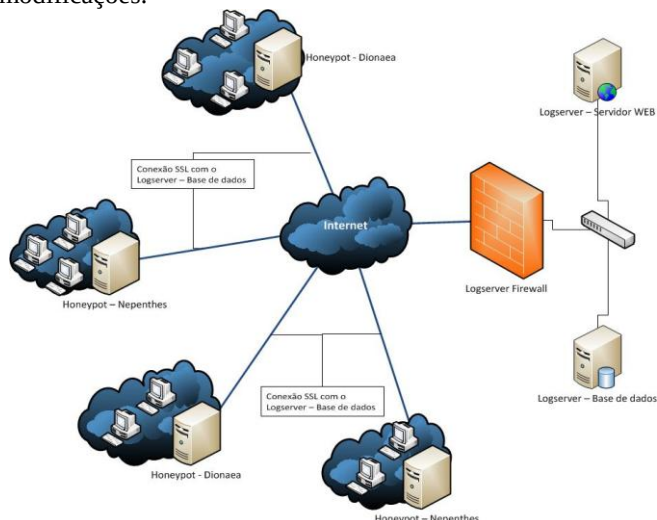


Fig. 2. Modelo de rede após alteração do SURFids

Observa-se na Figura 2 que os *Honeypots* ficam instalados na rede do cliente, com quantos endereços IP forem disponibilizados. Ao receber um acesso, esse é tratado como ataque.

O *Honeypot* irá tentar obter uma cópia do artefato e registrar as informações do ataque. Uma vez concluído o ataque, o *Honeypot* se comunica com a base de dados centralizada e verifica através do hash MD5 se o artefato já foi armazenado. Caso tenha sido armazenado, ele insere somente os dados obtidos do ataque, sem enviar o artefato. Caso não tenha sido armazenado, ele insere os dados do ataque e envia o artefato para análise.

Após estudo da arquitetura do SURFids, as alterações ficaram restritas à base de dados e ao programa utilizado para verificar os artefatos obtidos pelos *Honeypots*. Foram acrescentadas novas colunas, alterando as funções utilizadas pelo SURFids para inserir dados nas tabelas do banco, e foi modificada a forma como é executado o programa que verifica os artefatos capturados, passando a ser executado de hora em hora e não mais na captura do artefato pelo *Honeypot*.

Dessa maneira, quando surgir uma nova versão do SURFids pode-se atualizar sem a preocupação de ter que reescrever o código fonte do sistema.

VII. ESTUDO DE CASO

Para o estudo de caso, foi utilizado o ambiente disponibilizado pela Divisão de Segurança de Sistemas de Informação (DSSI), do Centro de Tecnologia da Informação Renato Archer (CTI), localizado na cidade de Campinas.

O estudo contou com três *Honeypots* já instalados e em funcionamento na instituição. Foi necessário um equipamento

adicional para servir de base de dados e servidor WEB onde foi instalado o coletor centralizado.

O estudo ocorreu no período de outubro de 2009 a junho de 2010, onde foi analisada a arquitetura padrão do SURFids e posteriormente a arquitetura modificada.

Por fazer parte do consórcio brasileiro de *Honeypots*, a DSSI tem o objetivo de reunir os artefatos capturados para análise, para poder determinar quais os tipos de ameaças que trafegam na internet brasileira.

VIII. RESULTADOS

Após a execução da abordagem proposta, foram obtidos os seguintes resultados:

- Houve uma redução de até 70% na utilização do link de comunicação com o coletor centralizado, comparado a arquitetura padrão do SURFids;
- Observou-se que houve um isolamento dos artefatos maliciosos de software em cada instituição, proporcionando maior segurança com relação à abordagem anterior;
- Com a descentralização dos *Honeypots*, o processamento dos ataques ficou distribuído, eliminando a necessidade de grande poder de processamento no *Honeypot* centralizado;
- Foi possível utilizar os *Honeypots* já em funcionamento, efetuando-se modificações de arquivos de configuração;
- Verificou-se que o Dionaea, registra 200% mais ataques que o Nepenthes trabalhando em paralelo na mesma rede.

Para verificar se a abordagem proposta não apresenta as restrições do Sistema SURFids, utilizamos a interface Web do SURFids para verificar que um sensor capturou dados com mais de um endereço IP, conforme se observa na Figura 3.

Após a integração dos *Honeypots* iniciou-se a ativação das funcionalidades do SURFids e monitoramento da coleta. Obtendo-se informações como as apresentadas na Figura 4, onde o artefato é verificado junto a quatro antivírus diferentes, demonstra-se que a alteração na forma de execução do programa que verifica os artefatos capturados não comprometeu sua funcionalidade e permitiu uma redução de custo, pois as instituições não têm mais a necessidade de adquirir licenças de antivírus para cada *Honeypot* instalado.

Na Figura 4 podemos visualizar que alguns artefatos não são identificados pelos antivírus utilizados e aparecem com o nome de "*suspicious*". A partir dessa informação pode-se concluir que esses artefatos podem vir a ser um novo vírus quando não identificados por nenhum dos antivírus, ou que a base de assinaturas utilizadas para identificar o artefato ainda não foi atualizada. Por esse motivo utiliza-se mais de um antivírus na análise.

Results (page 3: 40 - 60 of 596)

Timestamp	Severity	Source	Port	Destination	Port	Sensor	Additional info
27-05-2010 19:38:18	Malware downloaded	95.27.109.157		216.194		MAGNETO	Info
27-05-2010 19:38:15	Malware downloaded	95.27.109.157		216.193		MAGNETO	Info
27-05-2010 19:31:54	Malware downloaded	200.106.165.61		216.172		STORM	Info
27-05-2010 19:26:25	Malware downloaded	200.49.21.114		216.142		STORM	Info
27-05-2010 19:23:49	Malware downloaded	200.100.80.87		216.149		STORM	Info
27-05-2010 19:18:06	Malware downloaded	200.199.93.137		216.213		MAGNETO	Info
27-05-2010 19:14:47	Malware downloaded	200.100.164.236		216.167		STORM	Info
27-05-2010 19:10:43	Malware downloaded	200.49.17.119		216.186		STORM	Info
27-05-2010 19:07:21	Malware downloaded	95.27.109.157		216.221		MAGNETO	Info
27-05-2010 18:54:38	Malware downloaded	200.39.115.68		216.138		STORM	Info
27-05-2010 18:29:26	Malware downloaded	95.27.109.157		216.254		MAGNETO	Info
27-05-2010 18:29:18	Malware downloaded	95.27.109.157		216.253		MAGNETO	Info
27-05-2010 18:29:15	Malware downloaded	95.27.109.157		216.251		MAGNETO	Info
27-05-2010 18:29:13	Malware downloaded	95.27.109.157		216.249		MAGNETO	Info
27-05-2010 18:29:12	Malware downloaded	95.27.109.157		216.250		MAGNETO	Info
27-05-2010 18:29:05	Malware downloaded	95.27.109.157		216.248		MAGNETO	Info
27-05-2010 18:29:02	Malware downloaded	95.27.109.157		216.247		MAGNETO	Info
27-05-2010 18:28:53	Malware downloaded	95.27.109.157		216.244		MAGNETO	Info
27-05-2010 18:28:48	Malware downloaded	95.27.109.157		216.243		MAGNETO	Info
27-05-2010 18:28:43	Malware downloaded	95.27.109.157		216.242		MAGNETO	Info

Fig. 3. Download de artefatos de um mesmo sensor com endereços IP diferentes

Malware downloaded					
Malware	AV-1	AV-2	AV-3	AV-4	Stats
ba3a..	W32/Virut-54	Win32/Virtob	Worm/Korgo.A	W32/Virut.AX	203
7d99..	Worm.Padobot.M	Win32:Padobot-Y [Wrm]	Worm/Korgo.A	WORM/Korgo.Q	94
ca49..	Trojan.Small-4287	Win32:Virtob	Worm/Korgo.A	W32/Virut.AT	74
4847..	Worm.Padobot.M	Win32:Parite	Worm/Korgo.A	W32/Parite	35
57ad..	Worm.Allaple-2	Win32:Rbot-DQS [Trj]	Win32/Virut	W32/Virut.AX	23
c7d7..	Suspicious	Suspicious	Suspicious	Suspicious	19
0dfe..	Suspicious	Win32:Malware-gen	Worm/Generic.BFDX	WORM/Kolab.iad	15
f7c4..	Suspicious	Suspicious	Suspicious	Suspicious	11
7de3..	Suspicious	Suspicious	Suspicious	Suspicious	10
■■■■	■■■■	■■■■	■■■■	■■■■	■■■■
8fd4..	Worm.Allaple-75	Win32:Allaple [Wrm]	Worm/Allaple.L	W32/Virut.N.DR	1
total %	72 / 76 = 94 %	73 / 76 = 96 %	72 / 76 = 94 %	73 / 76 = 96 %	

Fig. 4. Artefatos verificados após coleta

Na ultima coluna da Figura 4, é possível verificar que o mesmo artefato aparece mais de uma vez, podendo ser oriundo de diferentes *Honeypots*. Podemos visualizar essa situação na Figura 3, onde um único *hash* MD5 foi obtido de varias fontes.

IX. CONCLUSÕES

Como apresentado, a abordagem proposta permitiu obter uma visualização detalhada dos ataques e dos artefatos coletados, auxiliando o administrador da rede a tomar as decisões que visam proteger os dados da instituição.

Como resultados verificados, podem-se citar a redução de até 70% na utilização do link de comunicação, o aumento da segurança, pois houve um isolamento dos artefatos maliciosos de software em cada instituição, além do aumento dos registros de ataques.

Com a união de vários *Honeypots* espalhados por diversas instituições publicas e privadas, podemos obter um mapeamento das atividades maliciosas direcionadas às instituições brasileiras, orientando os administradores das redes participantes a tomarem medidas preventivas para garantir a segurança nacional.

REFERÊNCIAS

- [1] SURFnet. SURFids Home Page. 2010. Disponível em: <http://ids.surfnet.nl>. Acesso em: 02/03/2010.
- [2] Provos, N.; Holz, T. Virtual honeypots. Boston: Pearson Education Inc. 2007.
- [3] Carnivore.it. Nepenthes Development Team Home Page. 2010. Disponível em: <http://nepenthes.carnivore.it/>. Acesso em: 05/02/2010.
- [4] Carnivore.it. Dionaea Development Team Home Page. 2010. Disponível em: <http://dionaea.carnivore.it/>. Acesso em: 05/02/2010.
- [5] Eadz Consulting. Knoppix English Home Page. 2010. Disponível em: <http://www.knoppix.net/>. Acesso em: 16/04/2010.
- [6] OpenVPN Technologies. OpenVPN Home Page. 2010. Disponível em: <http://www.openvpn.net/>. Acesso em: 15/02/2010.
- [7] PostgreSQL Global Development Group. PostgreSQL Home Page. 2009. Disponível em: <http://www.postgresql.org/>. Acesso em: 16/11/2009.
- [8] Safaa O.; et al. Intrusion Detection alarms reduction using root cause analysis and clustering. Elsevier Journal of Computer Communications. Novembro de 2008.
- [9] García-Teodoro, P.; Díaz-Verdejo, J.; Maciá-Fernández, G.; Vázquez E. Anomaly-based network intrusion detection: Techniques, systems and challenges Elsevier Journal of Computer & Security. Agosto de 2008.
- [10] Zhonglin, Z. Intrusion Detection System Based on Fuzzy Choose-closed Principle. IEEE Sixth International Conference on Fuzzy Systems and Knowledge Discovery. 2009.