UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
INSTITUTO DE MATEMÁTICA

RAFAEL OLIVEIRA DOS SANTOS

Segurança da Informação na graduação: Proposta de criação de disciplina optativa sobre Análise de Malware

Prof. Valeria Menezes Bastos, D.Sc.
Orientador

Rio de Janeiro, Dezembro de 2016

Segurança da Informação na graduação: Proposta de criação de disciplina optativa sobre Análise de Malware

Rafael Oliveira dos Santos

Projeto Final de Curso submetido ao Departamento de Ciência da Computação do Instituto de Matemática da Universidade Federal do Rio de Janeiro como parte dos requisitos necessários para obtenção do grau de Bacharel em Ciência da Computação.

Apresentado por:

Rafael Oliveira dos Santos

Aprovado por:

Prof. Valeria Menezes Bastos, D.Sc.

Prof. Claudio Miceli de Farias, D.Sc.

Prof. Paulo Henrique de Aguiar Rodrigues, D.Sc.

Prof. Maria Luiza Machado Campos, D.Sc

RIO DE JANEIRO, RJ - BRASIL

Dezembro de 2016

Agradecimentos

Quero agradecer, em primeiro lugar, a Deus, e a minha família por toda força e apoio para a realização deste sonho.

RESUMO

Segurança da Informação na graduação: Proposta de criação de disciplina optativa sobre Análise de Malware

Rafael Oliveira dos Santos

Dezembro/2016

Orientador: Valeria Menezes Bastos, D.Sc.

Dentro da área da Segurança da Informação, um *malware*, abreviação do inglês para *malicious software* (programa malicioso), é qualquer programa que realiza atividades que causam algum dano ao usuário, ao computador, ou a rede. Recentemente, estatísticas apontam que o Brasil tem tido um papel importante na produção de *malwares* para o mundo. De igual modo, o número de brasileiros vítimas destes códigos maliciosos tem crescido consideravelmente. Uma possibilidade para reverter este quadro seria compreender a importância de uma Análise de *Malware* e suas principais atividades/procedimentos. O objetivo desta pesquisa é discutir a necessidade e formulação de uma disciplina optativa sobre Análise de *Malware* no contexto de um Curso de Ciência da Computação no Brasil, tendo como estudo de caso o Departamento de Ciência da Computação da UFRJ. Mediante toda proposta de referências, conteúdo programático, cronograma, e critérios de avaliação, foi feita uma avaliação para determinar o quão viável é inserir tal disciplina eletiva na grade curricular do curso de Bacharel de Ciência da Computação do DCC-UFRJ. Conclui-se que é possível a inserção de uma disciplina eletiva sobre Análise de *Malware* dentro da gradução a curto ou médio prazo a fim contribuir para a formação de profissionais na área de conhecimento.

ABSTRACT

Segurança da Informação na graduação: Proposta de criação de disciplina optativa sobre Análise de Malware

Rafael Oliveira dos Santos

Dezembro/2016

Advisor: Valeria Menezes Bastos, D.Sc.

In the information security field, a malware, abbreviation of malicious software, is any code that performs activities that may cause any harm to the user, computer, or network. Recently, statistics show that Brazil has had an important role in the production of malwares for the world. Likewise, the number of brazilian victims of these malicious codes has grown substantially. One possibility to reverse this cenario is understand the importance of a Malware Analysis and its main activities/procedures. The goal of this research is to discuss the need and formulation of a optional discipline about Malware Analysis in the context of a Computer Science course in Brazil, having the Computer Science Department of Federal University of Rio de Janeiro (UFRJ) as a case study. Through all the suggestion of references, program content, schedule, and rating criteria, it was made an evaluation to validate if it is possible include such discipline inside de Computer Science course of UFRJ. It is concluded that it is possible the inclusion of a course of Malware Analysis in a short to medium term in order to contribute to the training of professionals on this knowledge area.

Lista de Figuras

Lista de Tabelas

Sumário

Capítulo 1

Introdução

Uma informação pode ser definida como um conjunto organizado de dados que constitui uma mensagem sobre um determinado fenômeno ou evento (CONCEITO, 2011). Para prover segurança a determinada informação, é necessário atender três grandes pilares: (i) Confidencilidade, necessidade de garantir que as informações sejam divulgadas somente para aqueles que possuem autorização para vê-las; (ii) Integridade, necessidade de garantir que as informações não tenham sido alteradas acidentalmente ou deliberadamente, e que elas estejam corretas e completas e a (iii) Disponibilidade, que é a necessidade de garantir que os propósitos de um sistema possam ser atingidos e que ele esteja acessível àqueles que dele precisam (HOEPERS, STEDING-JESSEN, 2016). Infelizmente, existem diversos meios que podem ferir tais pilares, sendo um dos mais relevantes o chamado *malware*, abreviação do inglês de *malicious software* (programa malicioso, em português).

Um *malware* é um programa que faz qualquer atividade danosa ao usuário, ao computador, ou a uma rede (SIKORSKI, HONIG, 2012). Dentre suas categorizações mais famosas, é possível mencionar: (i) vírus, programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos; (ii) *worm*, programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador; (iii) *bot*, programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente; (iv) *spyware*, programa

projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros; (v) *backdoor*, programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim; (vi) cavalo de troia (*trojan)*, programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário, e (vii) *rootkit*, um conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido (CERT.BR, 2012).

Ainda se discute sobre qual foi o *malware* pioneiro desenvolvido na história, contudo, um dos primeiros a chamarem atenção de todo o mundo foi o *Morris Worm*, em 1988. O código malicioso, escrito pelo estudante da Universidade de Cornell na época Robert Tappan Morris, consumia muito recurso computacional, criava cópia de si mesmo, e acabou infectando aproximadamente 10% dos computadores que estavam contectados na *Internet* (KELTY, 2016). Em 2010, o *Stuxnet Worm* foi um outro exemplo famoso de código malicioso, ao que muitos fatores indicam, feito por governos e que tinha como finalidade infectar usinas nucleares iranianas (SCHNEIER, 2010). Trazendo a história um pouco mais para o território nacional, o Brasil nos últimos anos tem sido um campo muito fértil para a criação de *malwares* bancários, códigos maliciosos voltados para instituições financeiras, dadas as estatísticas mais recentes descritas na Tabela 1.1. Evidenciando este fato, *malwares* brasileiros têm apresentado diversas técnicas avançadas de desenvolvimento, tornando-os mais difícieis de serem detectados e combatidos (MARQUES, 2016). Antes fáceis de serem analisados e tratados, por conta da falta de técnicas como por exemplo ofuscação de código, os códigos maliciosos do Brasil analisados recentemente atestam um grande avanço de sofisticação em suas produções. Agravando este cenário, diversas oportunidades ilícitas são oferecidas no mercado negro digital brasileiro para treinamento *online* de produção de *malwares* (MERCÊS, 2015).

No ponto de vista das organizações que precisam lidar com tais ameaças, existem alguns procedimentos que podem ser realizados por um time especializado em Segurança da Informação com o intuito de mitigar ou, no melhor caso, erradicar

Posição	**País**	**% de usuários atacados**
1	Turquia	3,45
2	Russia	2,92
3	Brasil	2,63
4	Paquistão	2,60
5	Venezuela	1,66
6	Tunísia	1,62
7	Japão	1,61
8	Singapura	1,58
9	Líbia	1,57
10	Argentina	1,48

Tabela 1.1: Lista da porcentagem de usuários de *internet banking* atacados por *malwares*. Adaptado de (UNUCHECK, et al., 2016)

os cenários adversos criados por códigos maliciosos (CERT, 2016). Dentre eles, é possível citar a Análise de *Malware* que pode ser descrita como a arte de dissecar programas maliciosos com o intuito de entender como funcionam, como identificá-los, como vencê-los, e como eliminá-los (SIKORSKI, HONIG, 2012). A formação de profissionais capazes de atuar nesta área poderia trazer enormes benefícios para organizações, pois estariam preparados a lidar com eventos adversos causados por *malwares*, assim como de uma certa forma contribuir para uma *Internet* brasileira mais segura.

As universidades brasileiras, principais formadoras de profissionais da área de tecnologia e informação, precisam seguir regularmente as diretrizes curriculares definidas pelo Ministério da Educação (MEC) em suas grades curriculares e, ao analisar o documento mais recente que mostra tais caminhos, tópicos sobre Segurança da Informação não são muito bem definidos, sendo descritos somente como "Segurança" (MEC, 2003). A Sociedade Brasileira de Computação (SBC), uma Sociedade Científica sem fins lucrativos com 38 anos de atuação, que reúne estudantes, professores, profissionais, pesquisadores e entusiastas da área de Computação e Informática de todo o Brasil (SBC, 2016), também divulga regularmente um currículo de referência para cursos de graduação em Computação e Informática, e, em seu documento mais recente (SBC, 2005), o tópico "Segurança e Auditoria de Sistemas" é definido como um assunto relevante a ser lecionado. Mediante tais definições, (MEC, 2003) e (SBC, 2005), é possível perceber que a Segurança da Informação já é considerada um tema importante a ser abordado e, apesar da inexistência de disciplinas de segurança na graduação de Bacharel em Ciência da Computação no Departamento de Ciência da Computação da Universidade Federal do Rio de Janeiro (SIGA, 2016 e Figura 1.1), a Universidade já possui esforços de abordagem ao tema, sendo o Grupo de Resposta a Incidentes de Segurança (GRIS-UFRJ) um dos exemplos mais relevantes.

Formado em 2003 integralmente por alunos para suprir a carência de abordagem em Segurança da Informação, a missão maior do GRIS, como projeto do Departamento de Ciência da Computação, é oferecer orientação e suporte acadêmico aos alunos do curso de Bacharelado em Ciência da Computação do Departamento de Ciência da Computação da UFRJ, sem fins lucrativos, no que tange a temática da

Figura 1.1: Grade curricular de 2016 para o curso de Ciência da Computação da UFRJ

Segurança da Informação em todas as suas vertentes, nos âmbitos de ensino, pesquisa e extensão, e este é o principal, senão único, critério de orientação para questões internas e externas (GRIS, 2016). O grupo, composto em média por 15 alunos a cada semestre, é internamente dividido em três áreas: (i) Ensino, Desenvolvimento e Pesquisa (EDP), destinada à pesquisa teórica e prática de tecnologias e conceitos relacionadas a segurança da informação; elaboração de artigos, material didático e desenvolvimento de ferramentas de segurança; levantamento e, quando necessário, desenvolvimento de soluções e frameworks que as demais áreas necessitem, mediante solicitação. Área também responsável pela organização dos cursos, simpósios, workshops, palestras e mesas-redondas assim como a participação dos membros em eventos relacionados a segurança da informação; (ii) Redes, Sites e Sistemas (RSS), responsável pela instalação, configuração e administração de sistemas locais e remotos de uso/ responsabilidade do GRIS; administração do site do GRIS; elaboração de projetos de pesquisa e produção de artigos, material didático e cursos em geral relacionados à sua área de especialização, e (iii) Respostas a Incidentes e Auditoria (RIA), responsável pela realização de atividades de campo com os membros do GRIS em tarefas relacionadas à detecção, resolução e prevenção de incidentes de segurança da informação em quaisquer unidades solicitantes da UFRJ, sem custo algum para a solicitante; elaboração de projetos de pesquisa e produção de artigos, material didático e cursos em geral relacionados à sua área de especialização, para

uso interno e externo (GRIS, 2016).

Dentre alguns projetos produzidos pelo GRIS, é possível citar: (i) Segurança em Códigos QR, artigo que procura explicar com detalhes como funcionam os Códigos QR, mostrar até que ponto é seguro escaneá-los, exemplificar como alguns ataques podem ser feitos através de um estudo de caso, e por fim demonstrar algumas boas práticas na utilização dos mesmos (SANTOS, 2013); (ii) Labrador (também conhecido por *Labrador Intrusion Detection* ou *labrador-ids*), uma ferramenta multiplataforma criada para identificar quaisquer modificações indesejadas realizadas em um sistema, podendo ser utilizada como um verificador de integridade e como um *Intrusion Detection System* (IDS) (LABRADOR, 2007); e (iii) *Workshop-GRIS-UFRJ*, projeto no qual o grupo promove apresentações regulares dentro da Universidade a fim de promover a SI aos estudantes e funcionários, envolvendo diversos tópicos de segurança como a Computação Forense, Tratamento de Incidentes, Criptografia, Engenharia Reversa, entre outros (WORKSHOP GRIS, 2016).

O objetivo maior do autor desta pesquisa é apresentar ao DCC-UFRJ um possível conteúdo a ser lecionado em Segurança da Informação a fim de suprir ainda mais a carência de disciplinas na área, presenciada infelizmente há anos no curso. Apesar de ser um tema desafiador, este trabalho sugere a definição da disciplina "Análise de Malware"que servirá como pontapé inicial dentro da área de Segurança da Informação, sendo uma disciplina que contém diversos tópicos relevantes ao conhecimento dos alunos. Além disso, este trabalho apresenta sugestões de ementa, referências, conteúdo programático, cronograma, exercícios práticos, e critérios de avaliação.

O restante do trabalho se divide em outros três capítulos. O Capítulo 2 serão mostrados conceitos básicos necessários ao entendimento da proposta deste projeto e apresenta uma análise sobre como esse tema é abordado nas principais universidades do Brasil e do mundo. O Capítulo 3 descreve toda a proposta da disciplina Análise de Malware. E finalmente o Capítulo 4 traz as conclusões obtidas e aponta direções futuras.

Capítulo 2

Conceitos básicos

Esse capítulo apresenta os principais conceitos sobre os quais a proposta do presente trabalho se baseia. A seção 2.1 define as etapas para a inclusão de uma disciplina na UFRJ. A seção 2.2 mostra os princípios do processo de Tratamento de Incidentes, uma atividade onde uma Análise de Malware pode estar associada. A seção 2.3 mostra uma análise de algumas universidades internacionais e nacionais sobre como a abordagem em segurança é feita dentro da graduação em Ciência da Computação.

2.1 Inclusão de disciplina na UFRJ

O Conselho de Ensino de Graduação (CEG) da Universidade Federal do Rio de Janeiro é o órgão colegiado deliberativo em matéria didática e pedagógica, que traça as diretrizes para a orientação e normatização das atividades acadêmicas e participa da elaboração e implementação das linhas de ação que visam à melhoria da qualidade do ensino, define a política acadêmica dos cursos, fixando as normas de ensino dos cursos de graduação e das formas de ingresso na UFRJ (CEG, 2003). De acordo com CEG, uma disciplina é um conjunto de atividades acadêmicas, organizadas didático-pedagogicamente, versando sobre matéria determinada, com carga horária definida, local e horário próprios para realização, de execução restrita a um período letivo e exigências de avaliação definidas no currículo, cujo cumprimento se traduza

por grau.

Na mesma resolução (CEG, 2003), fica definida como uma disciplina optativa aquela integrante de uma área de conhecimento, consignada no currículo, dentre os quais o aluno tenha que escolher algum ou alguns para completar determinado número de créditos, podendo o currículo estabelecer condições limitadoras da escolha de modo que, no conjunto, as disciplinas e requisitos curriculares suplementares escolhidos formem um grupo concatenado.

Tendo ainda (CEG, 2003) com referência, a criação de disciplinas deve ser de iniciativa do departamento responsável pelo conteúdo. Portanto, apesar de esta pesquisa sugerir uma proposta de inclusão de uma disciplina optativa dentro da graudação em Ciência da Computação na UFRJ, cabe ao DCC-UFRJ avaliar minuciosamente a sugestão, e caso a julgue válida, ser o responsável em incluí-la na grade curricular do curso em questão.

2.2 Tratamento de Incidentes

Um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores(CERT.BR FAQ, 2016). Caso ocorram, incidentes devem ser analisados minuciosamente por uma equipe de segurança a fim de mitigar ao máximo os danos eventualmente causados. Para tal, é definido o processo de Tratamento de Incidentes que deve estar associado a quatro grandes etapas: (i) Preparação; (ii) Detecção e Análise; (iii) Contenção, Erradicação, e Recuperação, e (iv) Atividades Pós-incidente (NIST, 2012).

A etapa de inicial envolve estabelecer e treinar um time de resposta a incidentes, e adquirir as ferramentas e recursos necessários. Durante a Preparação, a organização procura também limitar o número de incidentes que irão acontecer ao selecionar e implementar um conjunto de procedimentos baseados nos resultados de uma análise prévia de riscos. Algumas das considerações importantes nesta fase envolvem preparar *notebooks* para o time de segurança, organizar uma lista de contatos internos e

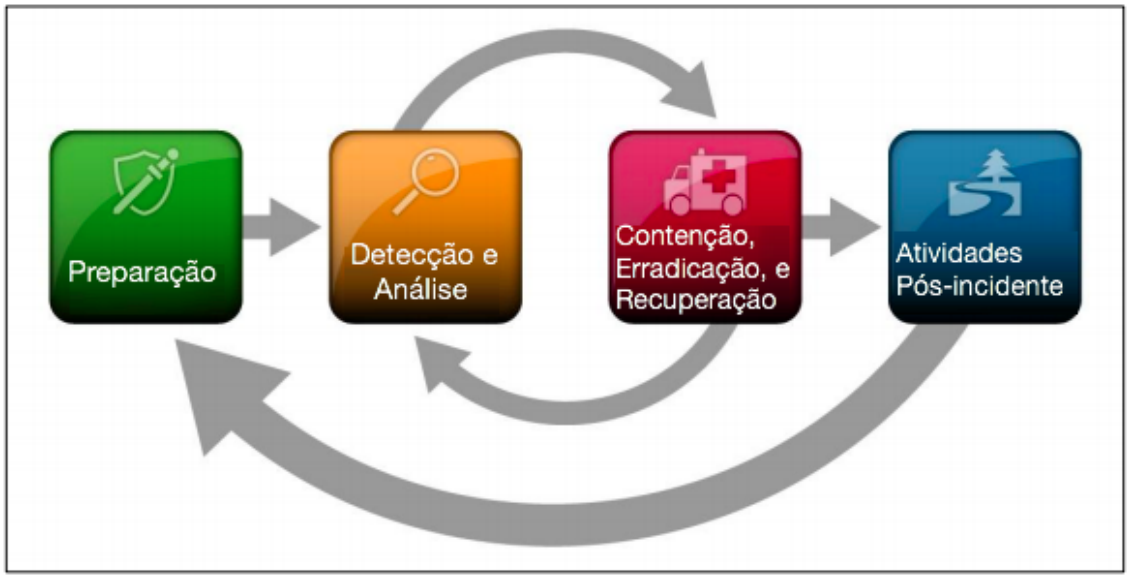

Figura 2.1: Fluxograma de um Tratamento de Incidentes. Adaptado de referencia26

externos, ter em mãos documentação dos protocolos, aplicações, e outros prodrutos utilizados, preparar uma *War Room*, um ambiente reservado para reuniões com os membros do time para definição de estratégias, entre outros.

A etapa de Detecção e Análise é necessária para alertar a organização sempre que um incidente acontecer assim como para analisá-lo quando necessário. De acordo com a gravidade do incidente, é possível mitigar o impacto e em seguida se recuperar dele, e quanto mais bem preparada a equipe de segurança e a organização estejam, mais rápido será o tratamento do mesmo. Durante esta fase, a detecção de indicadores e precursores, configuração de mecanismos de defesa, criação de políticas de retenção de logs, **Análise de Malware** (grifo meu), correlação de eventos, são algumas das atividades importantes que podem citadas.

A terceira fase é onde a resposta ao incidente de fato será dada. O primeiro passo sempre deve ser a contenção do incidente, evitando que o mesmo se espelhe ainda mais, consequentemente causando mais danos a organização. Na medida que a equipe de segurança ateste que uma eventual ameaça está de fato controlada, se faz necessário realizar alguns procedimentos para erradicar o problema, como por exemplo deletando *malwares*, desabilitando contadas comprometidas, identificando as vulnerabilidades exploradas em outros computadores, entre outros. Finalizando

a etapa, a Recuperação serve para restaurar o ambiente ao seu estado normal de operação, tendo a restauração completa do sistema, troca de senhas, instalação de *patchs*, formatação de discos comprometidos, algumas das etapas que podem ser seguidas.

A última etapa chamada de Atividades Pós-incidente pode também ser descrita como Lições Aprendidas. Aqui, questionamentos como "O que exatamente ocorreu?", "Quais foram as etapas até a recuperação?", "Quais ações devem ser feitas caso aconteça denovo?", entre outros precisam terem suas respostas bem definidas e, o mais importante, bem documentadas. O quão mais madura e solidificada esta fase estiver dentro de um processo de Tratamento de Incidentes, mais fácil pode ser para evitar futuros incidentes que já aconteceram previamente dentro de uma organização.

2.3 Universidades internacionais e nacionais que abordam segurança na graduação

Conhecer e entender como a segurança da informação é vista nas universidades permite à UFRJ ter ponteciais referências para a abordagem no tema, assim como a traçar principais estratégias para melhorar o quadro atual. De tal forma, algumas das melhores universidades para o curso de Ciência da Computação no Brasil e ao redor do mundo, de acordo com (QS, 2016), foram escolhidas para uma análise da abordagem em segurança.

2.3.1 Universidades internacionais

O *Massachusetts Institute of Technology* (MIT), universidade americana privada localizada em Cambridge, possui uma boa abordagem em Segurança da Informação a graduação através das seguintes disciplinas: (i) "Computer Systems Security", em português Segurança em Sistemas Computacionais, aborda temas como *Buffer Overflow*, ataques de roubo de sessão, escalação de privilégios, segurança em *Android*, segurança em aplicações *web*, e segurança em redes (KAASHOEK; MORRIS,

2016), e (ii) "Computer and Network Security", em português Segurança em Redes e Computadores, é focada em temas da Criptografia como *One-time pad*, funções *hash*, cifras criptográficas, *El gamal*, assinaturas digitais, RSA (RIVEST, 2016).

A *Stanford University*, universidade americana privada localizada na Californa, possui uma excelente abordagem sobre segurança através das seguintes três disciplinas: (i) "Computer and Network Security", em português Segurança em Redes e Computadores, com temas em segurança em Sistema Operacionais, técnicas de exploração e *fuzzing*, segurança em aplicações *web*, visão geral sobre criptografia, segurança em redes, e ataques de negação de serviço (BONEH; MITCHEL, 2016); (ii) "Web Programming and Security", em português Programação *Web* e Segurança, a disciplina mostra como se estrutura a programação para aplicações *web* juntamente com tópicos de segurança para um desenvolvimento seguro (BONEH; et al., 2009), e (iii) "Introduction to Cryptography", em português Introdução à Criptografia, assiciando tópicos de tal área de conhecimento com a segurança da informação, como por exemplo criptografia simétrica, integridade de mensagens, criptografia de chave pública, e assinatura digital (HARRIS, 2016).

A universidade americana *Carnegie Mellon University* localizada no estado da Pensilvânia também possui uma boa abordagem de segurança na graduação através das seguintes disciplinas: (i) "Information Security and Privacy", em português Segurança da Informação e Privacidade, com temas como definição sobre cibercrime, segurança em dispositivos móveis, privacidade e *big data*, e segurança em protocolos (SADEH, 2016), e (ii) "Introduction to Computer and Network Security and Applied Cryptography", em português Introdução a Segurança em Redes e Computadores e Criptografia aplicada, que busca mostrar os princípios básicos de segurança, tópicos em criptografia simétrica e assimétrica, e segurança em redes (PERRIG, 2016).

2.3.2 Universidades nacionais

A Universidade de São Paulo (USP) possui uma abordagem básica em segurança através da disciplina chamada "Criptografia para Segurança de Dados" (JÚPITER, 2016). Nela, a criptografia é transmitida com o seguinte conteúdo programático: (i)

Métodos tradicionais de criptologia; (ii) Teoria da informação; (iii) *Data Encryption Standard* (DES) e *Advanced Encryption Standard* (AES), e (iv) Sistemas de distribuição de chaves públicas e secretas.

A Universidade de Campinas (UNICAMP) possui uma boa abordagem em seu curso de Ciência da Computação dada a disciplina oferecida chamada "Programação Segura e Análise de Malware" (ARANHA, 2015). Dentre alguns dos temas, é possível citar: (i) *Worms, Backdoors, Trojans*; (ii) *Phishing Trojans*, introdução à Criptografia; (iii) Análise Estática e Dinâmica de *malwares*; (iv) Métodos de autenticação; (v) Segurança em aplicações *web*, e (vi) vulnerabilidades de *software*.

A Pontifícia Universidade Católica do Rio de Janeiro (PUC-RIO) possui uma abordagem básica em segurança na graduação através da disciplina "Segurança da Informação" (SILVA, 2016). A ementa do curso engloba os seguintes tópicos: (i) Princípios em segurança da informação; (ii) Análise de Riscos; (iii) Leis, normas e padrões de segurança da informação; (iv) Auditoria de sistemas; (v) Autenticação e controle de acesso; (vi) Aspectos tecnológicos da segurança da informação; (vii) Plano de continuidade do negócio, e (viii) Boas práticas em segurança da informação.

Capítulo 3

Proposta

Esse capítulo apresenta a proposta do presente trabalho, a elaboração de uma disciplina eletiva sobre Análise de Malware a ser possivelmente incluída na graduação do curso de Bacharel em Ciência da Computação no DCC-UFRJ. A seção 3.1 apresenta o título e descrição do curso. A seção 3.2 detalha quais são os objetivos da disciplina. A seção 3.3 detalha uma possível ementa juntamente com o conteúdo programático. A seção 3.4 define as atividades quem podem complementar as aulas teóricas. A seção 3.5 discute possíveis referências que auxiliem os estudos em Análise de Malware. A seção 3.6 detalha a importância de Monitoria e como alunos do GRIS-UFRJ podem auxiliar no andamento da disciplina. A seção 3.7 mostra uma possível agenda para os tópicos propostos. A seção 3.8 mostra os pré-requisitos para o bom entendimento da disciplina. E finalmente, a seção 3.9 mostra quais podem ser possíveis critérios de avaliação para a disciplina Análise de Malware.

3.1 Título e descrição do curso

Dado que o tema a ser lecionado se chama Análise de Malware, fica definido como o melhor título para a disciplina o próprio nome da área de conhecimento: Análise de Malware. Se baseando ainda nas motivações e definições descritas neste documento, uma possível descrição para tal curso incluiria as seguintes afirmações: "O crescimento de avanços tecnológicos e a facilidade de acesso à informação tornam

a Internet um campo fértil para a proliferação em massa de *malwares*. Este fato se justifica aqui no Brasil na medida que a conscientização da Segurança da Informação não consegue evitar que o número de infecções de códigos maliciosos nos dispositivos crescam diariamente. De acordo com estatísticas recentes de empresas importantes na área da Segurança da Informação, o Brasil tem um papel considerável na criação de programas maliciosos para todo o mundo. Como resultado, a habilidade de detectar, analisar, entender, controlar, e erradicar *malwares* são questões que devem ser vistas com urgente importância pelo bem da economia e segurança nacional. Esta disciplina irá debater as técnicas modernas para Análise de Malware através de documentos e exercícios práticos com exemplos reais encontrados na Internet."

3.2 Objetivo

Após a conclusão desta disciplina, o aluno deverá ter os conhecimentos necessários para analisar sofisticados *malwares*, utilizando tanto a Análise Estática quanto a Análise Dinâmica. Sendo mais específico nos tópicos, o estudante (i) irá adiquirir um conhecimento aprofundado sobre os formatos executáveis, *Windows Internals*, assim como a *Application Programming Interface* (API) do Windows; (ii) será capaz de extrair informações relevantes de um *host* e indicadores de rede que estejam eventualmente associados a um programa malicioso; (iii) conseguirá aplicar as técnicas e conceitos sobre *unpack*, extrair, descriptografar, ou contornar novas técnicas de anti-análise nas futuras amostras de *malwares*; (iv) alcançará proficiência em ferramentas como IDA Pro, OllyDbg, WinDBG, PE Explorer, ProcMon, entre outras.

3.3 Ementa e conteúdo programático

A ementa sugerida para a disciplina Análise de *Malware*, que estará apresentada também no Apêndice B, fica divida em 9 aulas teóricas: (i) Introdução e Análises Básicas; (ii) Análise Estática Avançada; (iii) Análise de programas do *Windows*; (iv) Análise Dinâmica Avançada e (*Debugging*); (v) Comportamentos de *malwares*; (vi) Codificando e Decodificando informações; (vii) Técnica Covert Launching; (viii)

Anti-análise, e (ix) *Packer* e *Unpacking*.

A primeira aula deve estabelecer uma visão geral sobre o processo e metodologia da Análise de *Malware*, ensinar formas para colher informações de um executável sem executá-lo, mostrar como um ambiente seguro deve ser configurado a fim de executar um código malicioso, assim como ensinar técnicas fáceis, porém efetivas, para analisar um *malware* ao executá-lo. Um pequeno exemplo de *slides* para uma parte da aula introdutória está disponível mais adiante no Apêndice A. Dividindo a aula em tópicos sugeridos: (i) Definições sobre *malwares*; (ii) Motivações para desenvolver um código malicioso; (iii) Histórico dos *malwares*; (iv) Definições sobre Análise de *Malware*; (v) Técnicas para a Análise Estática Básica; (vi) Como configurar um ambiente seguro, e (vii) Técnicas para a Análise Dinâmica Básica.

A segunda aula é dedicada à Análise Estática Avançada, fazendo uma introdução à linguagem *assembly x86*, mostrando a ferramenta *IDA Pro*, uma das mais importantes ferramentas para Análise de *Malware*, e detalhando alguns exemplos de programas em C escritos na linguagem *assembly*. Dividindo a aula em tópicos sugeridos: (i) Níveis de abstrações das linguagens de programação; (ii) Definições sobre Engenharia Reversa; (iii) Instruções, Operandos, Registradores, e *Flags* (x86); (iv) Definições sobre a ferramenta *IDA Pro*; (v) Interface, Navegação, Pesquisando, Gráficos, e *Plugins* do *IDA Pro*; (vi) Analisando códigos em C no *IDA Pro*.

A terceira aula deve cobrir conceitos específicos do sistema operacional (SO) *Windows* que são necessários para o entendimento de programas maliciosos desta natureza. Dividindo a aula em tópicos sugeridos: (i) API do *Windows*; (ii) Registros do *Windows*; (iii) APIs de Rede, e (iv) Definições sobre *Dynamic Link Library* (DLL), Processos, *Threads*, Serviços, textitMicrosoft Component Object Model (COM), e *Exceptions*.

A quarta aula é responsável em abordar a Análise Dinâmica Avançada, explicando os conceitos básicos da técnica chamada de *debugging* e detalhar como analistas de *malware* podem usar um *debugger*. Dividindo a aula em tópicos sugeridos: (i) Definições sobre o *debugging*; (ii) Diferentes técnicas de *debug*; (iii) Definições sobre *Breakpoints* e *Exceptions*; (iv) Modificando execução de um programa com

um *debugger*, e (v) definições sobre as ferramentas *WinDbg* e *OllyDbg*.

A quinta aula descreve funcionalidades comuns de *malwares* e mostra como reconhecer tal comportamente ao analisar um *malware*. Dividindo a aula em tópicos sugeridos: (i) *Downloaders* e *Launchers*; (ii) *Backdoors*; (iv) *Credential Stealers*; (v) Mecanismos de Persistência, e (vi) Escalação de Privilégios.

A sexta aula deve demostrar como um *malware* consegue codificar informações a fim de tornar sua identificação mais difícil, assim como mostrar técnicas para fazer o processo inverso de decodificação. Dividindo a aula em tópicos sugeridos: (i) Objetivos de analisar algoritmos de codificação; (ii) Cifras Simples; (iii) Algoritmos comuns de Criptografia; (iv) Esquemas de codificação customizáveis, e (v) Técnicas para a decodificação.

A sétima aula deve discutir como analisar classes "escondidas" de *malwares* que têm como finalidade esconder suas próprias execuções dentro de outros processos, técnica esta chamada de *Covert Launching*. Dividindo a aula em tópicos sugeridos: (i) Definições sobre *Launchers*; (ii) Injeção de processos; (iii) Substituição de processos; (iv) Injeções *Hook*, e (v) Injeções *Asynchronous Procedure Call* (APC).

A oitava aula deve procurar mostrar como funciona a Anti-análise, técnica utilizada por desenvolvedores de *malwares* para atrasar ou previnir a análise de seus códigos maliciosos. Dividindo a aula em tópicos sugeridos: (i) *Anti-Dissassembly*; (ii) *Anti-Debugging*; (iii) *Anti-Máquina Virtual*, e (iv) *Anti-Antivírus*.

A última aula deve mostrar ao aluno como *malwares* utilizam a técnica de *Packing* para esconder suas reais atividades maliciosas, e em seguida mostrar as técnicas inversas chamadas de *Unpacking*. Dividindo a aula em tópicos sugeriods: (i) Anatomia de um *packer*; (ii) Identificando programas *packed*; (iii) *Unpacking* automatizado; (iv) *Unpacking* manual, e (v) *Packers* mais comuns.

3.4 Atividades práticas

A fim de complementar o material teórico, os alunos devem realizar atividades práticas para cada aula sugerida, nomeadas aqui como laboratórios e projeto final. Os laboratórios podem envolver perguntas teóricas sobre o conteúdo passado, mas preferencialmente devem conter amostras de códigos maliciosos a serem analisados pelos alunos. Para exemplificar, um laboratório associado à aula 5 sobre *Comportamentos de malwares*, poderia questionar como um dado executável malicioso consegue coletar informações dentro do sistema afetado.

O Trabalho Final deve ser uma tarefa extra-classe, descrita ao decorrer do curso, e que procure englobar ao máximo os conhecimentos passados durante a disciplina. Por exemplo, pode-se pedir que os alunos se dividam em grupos pequenos, simulando serem uma equipe de segurança de uma instituição, a fim de analisar um *Advanced Persistence Threat* (APT) descoberto dentro da rede. O Projeto Final pode exigir também um modelo padrão para os relatórios, ensinando assim uma boa organização de documento aos alunos sobre Análises de *Malware*. É preciso porém, para ambas atividades, uma extrema atenção ao analisar arquivos potencialmente maliciosos, tendo em vista que executar um *malware* em um ambiente não seguro pode danificar seriamente os sistemas ou redes envolvidos. O docente responsável pela disciplina, caso julgue válido, pode tornar as aulas teóricas como opcionais aos estudantes. Contudo, fica definido que as atividades práticas são obrigatórias e imprescindíveis para a aprovação do aluno, conforme será descrito mais adiante em Critérios de avaliação.

3.5 Material sugerido para referências

O material sugerido como referência envolve quatro livros conceituados na área de Análise de *Malware*, sendo eles: (i) *Practical Malware Analysis*, 2012, por Michael Sikorski e Andrew Honig, recentemente premiado como livro do ano (4:cast, 2013), possui um extenso e rico conteúdo a fim de ensinar técnicas para análise, *debugging*, e *disassembling* de *malwares* de forma segura, podendo se tornar o li-

vro texto da disciplina aqui proposta; (ii) *Malware Analyst's Cookbook*, 2010, por Michael Ligh, Steven Adair, Blake Hartstein, e Matthew Richard, acompanhando uma mídia com exemplos práticos, procura cobrir tópicos cruciais que um analista de *malware* precisa saber no ponto de vista dos autores; (iii) *Practical Reverse Engineering*, 2014, por Bruce Dang, Alexandre Gazet, Elias Bachaalany, e Sébastien Josse, através de diversos exemplos práticos, este livro está associado fortemente à Engenharia Reversa, prática essencial para um analista de *malware*, podendo ser muito útil como um material de consulta aos alunos, e (iv) *The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System*, 2009, por Bill Blunden, livro com aproximadamente 900 páginas, aborda profundamente o funcionamento de *rootkits*, um tipo específico de *malware*, e pode ser indicado para os alunos que quiserem se aprofundar ainda mais no tema.

3.6 Monitoria

As aulas de Análise de *Malware* devem ser ministradas, sempre que possível, dentro dos laborários, tendo em vista que muitos exercícios práticos são sugeridos para uma melhor compreensão dos alunos. De tal forma, para ajudar o professor que lecionará o curso, é crucial que existam alunos responsáveis em montar os laboratórios e acompanhar as aulas práticas. Dado que o Departamento de Ciência da Computação possui o GRIS-UFRJ, alunos da Universidade que estudam Segurança da Informação, os membros deste grupo se enquadariam perfeitamente como monitores da disciplina. Fica definido como papel do monitor: (i) elaborar e atualizar os exercícios de laboratórios, com o aval do professor; (ii) auxiliar o professor durante as aulas de laboratórios; (iii) corrigir, juntamente com o professor, os laboratórios dos alunos, e (iv) auxiliar os alunos com o Trabalho Final, remota ou presencialmente nos laboratórios.

3.7 Carga horária e cronograma

Fica definida como carga horária deste curso um total de 60 horas, quantidade esta semelhante às outras disciplinas eletivas no curso de Bacharel em Ciência da Computação no DCC-UFRJ (SIGA, 2016). Adicionalmente, mediante ao conteúdo programático, aos laboratórios, e ao projeto final proposto anteriormente, o cronograma sugerido para a disciplina é descrito na tabela 2.1.

Dia	**Título**	**Tópicos**	**Horas**
1	Aula 1	Análise Estática Básica, Análise Dinâmica Básica	2
2, 3	Laboratório 1	Monitoria GRIS-UFRJ	4
4	Aula 2	Análise Estática Avançada	2
5, 6	Laboratório 2	Monitoria GRIS-UFRJ	4
7	Aula 3	Análise de programas do *Windows*	2
8, 9	Laboratório 3	Monitoria GRIS-UFRJ	4
10	Aula 4	Análise Dinâmica Avançada e *Debugging*	2
11, 12	Laboratório 4	Monitoria GRIS-UFRJ	4
13	Aula 5	Comportamentos de *malwares*	2
14, 15	Laboratório 5	Monitoria GRIS-UFRJ	4
16	Aula 6	Codificando e Decodificando informações	2
17, 18	Laboratório 6	Monitoria GRIS-UFRJ	4
19	Aula 7	Técnica *Covert Launching*	2
20, 21	Laboratório 7	Monitoria GRIS-UFRJ	4
22	Aula 8	Anti-análise	2
23, 24	Laboratório 8	Monitoria GRIS-UFRJ	4
25	Aula 9	*Packer* e *Unpacking*	2
26, 27	Laboratório 9	Monitoria GRIS-UFRJ	4
28	Aula 10	Tira dúvidas do projeto final	2
29, 30		Apresentação do Projeto Final	4
		Total de Horas	60

Tabela 3.1: Agenda sugerida para o curso Análise *Malware*

3.8 Pré-requisitos

Para a inscrição na disciplina Análise de Malware, se faz necessário que o aluno tenha concluído a disciplina Computadores e Programação (MAB353) na graduação em Bacharel em Ciência da Computação no DCC-UFRJ. Tal curso fornece uma base sólida sobre *Assembly*, uma visão sobre os conceitos de Engenharia Reversa, estrutura de processos, tratamento de exceção e interrupções, que são essenciais para o entendimento dos diversos temas propostos na nova disciplina.

3.9 Critérios de avaliação

A UFRJ define entre duas avaliações durante o período uma média mínima para aprovação de 7. Contudo, fica sugerido aqui como alternativa (caso aplicável), uma avaliação mediante as exercícios práticos dos laboratórios e projeto final: a soma de todas as notas do laboratórios, sendo a máxima 10 e mínima 0, deve representar 70% da notal final do aluno, enquanto a nota do Trabalho Final, sendo a máxima 10 e mínima 0, representa os restantes 30%.

Capítulo 4

Conclusão

Esse capítulo descreve a conclusão da pesquisa, fazendo uma avaliação de cada item proposto do capítulo anterior, assim como detalhando possíveis projetos futuros para a inclusão da disciplina Análise de Malware. A seção 4.1 mostra a avaliação feita sobre a ementa e o conteúdo programático. A seção 4.2 avalia o material sugerido para ser utilizado como referência. Na seção 4.3 são apresentadas as considerações sobre as atividades práticas. A seção 4.4 descreve a aplicabilidade da sugestão dos alunos do GRIS-UFRJ como monitores da disciplina. A seção 4.5 avalia a carga horária e o cronograma. A seção 4.6 descreve as avaliações dos pré-requisitos propostos. A seção 4.7 compara os critérios de avaliação propostos com alguns outros cursos dentro da graduação em Bacharel em Ciência da Computação do DCC-UFRJ. E, por fim, seção 4.8 descreve o desfecho da pesquisa juntamente com a definição de possíveis trabalhos futuros.

4.1 Ementa e conteúdo programático

As disciplinas de graduação em Bacharel em Ciência da Computação do DCC-UFRJ precisam ter definidas uma bibliografia a ser utilizada, incluindo um livro texto e referências complementares, conforme estipulado em (CEG, 2003). A ementa proposta no capítulo anterior foi baseada nos materiais sugeridos como referência na Seção 3.5, tendo como foco principal o livro *Practical Malware Analysis*, 2012, por

Michael Sikorski e Andrew Honig, sendo definido como livro texto para o curso. A ordem de tópicos descrita como conteúdo programático segue uma sequência similiar ao livro texto. Os outros livros também sugeridos como referências complementares também abordam de certa forma o conteúdo proposto, não restringindo assim o conteúdo programático somente ao livro texto.

4.2 Material sugerido para referências

Definido como livro texto, *Practical Malware Analysis*, é considerado referência para o assunto dentro da área de Segurança da Informação (4:cast, 2013). Como o próprio título do livro, todo conteúdo passado procura ser o mais prático possível, possuindo diversos exercícios de laboratório ao final de cada capítulo, assim como as soluções dos mesmos. Grande parte do conteúdo proposto na ementa do curso pode ser encontrado no livro, tornando-o sua aquisição pelo aluno altamente recomendável.

Mawlare Anlyst Cookbook possui em seu conteúdo diversos tópicos sugeridos na ementa da disciplina e pode ser utilizado também como referência de Análise de Malware. Os dois primeiros capítulos deste livro complementam o livro texto sugerido abordando tópicos sobre como tornar as atividades do analista de malware anônimas e seguras. Adicionalmente, também mostram como configurar um *Honeypot*, sistemas programados propositalmente para serem explorados, a fim de analisar amostras de *malwares*. *Mawlare Anlyst Cookbook* também acompanha uma mídia física contendo inúmeras amostras de códigos maliciosos para serem analisados, permitindo assim ao aluno uma gama maior de amostras a serem estudadas.

Apesar de *Pracital Reverse Engineering* não possuir todos os tópicos sugeridos como ementa do curso, o livro possui diversos fundamentos sobre a Engenharia Reversa que auxiliam enormemente ao analista de malware. Como exemplo, técnicas de ofuscação são debatidas e mostram como *malwares* conseguem previnir que ferramentas como anti-vírus detectem suas atividades maliciosas. Além disso, o livro também debate profundamente sobre o *Kernel* do *Windows*, permitindo ao aluno

entender como *rootkits* funcionam neste sistema operacional, por exemplo.

Para alunos que queiram se aprofundar ainda mais na Análise de Malware, o livro sugerido *The Rootkit Arsenal: Escape and Evasaion in the Dark Corners of the System* é uma ótima opção. O livro de mais de 900 páginas possui algumas semelhanças com a ementa proposta na disciplina, como por exemplo o capítulo onde detalha as técnicas de *Covert Channel*, além de abordar diversas outras técnicas que *rootkits* utilizam para se "esconder" dentro dos sistemas infectados.

4.3 Atividades práticas

É comum disciplinas dentro do curso de Bacharel em Ciência da Computação no DCC-UFRJ utilizarem exercícios práticos em laboratórios para auxiliar na absorção de conteúdos (AGUIAR, 2016). As atividades nos laboratórios, que representam o dobro do tempo das aulas teóricas, permitem aos alunos uma possibilidade muito maior de verem de fato como *malwares* funcionam na prática. Adicionalmente, os exercícios práticos a serem feitos e entregues para correção forçam o aluno a se dedicar e estar presente nos laboratórios, caso o contrário sua nota poderá estar comprometida. Com a atividade prática chamada de Trabalho Final, é possível afirmar que será muito enriquecedor para o aluno pois, através de uma simulação de um cenário adverso, ele estará preparado para eventos reais de ameaças que eventualmente poderá se deparar algum dia.

4.4 Monitoria

A monitoria sugerida sob responsabilidade dos membros do GRIS-UFRJ pode ser benéfica tanto para estes alunos quanto para o docente responsável pela disciplina. Os estudantes que compõem o grupo sempre sentiram a necessidade de terem disciplinas em segurança ao longos dos anos, e, ter a possibilidade de auxiliarem na cadeira em Análise de *Malware* seria extramemente enriquecedor para a suas formações profissionais na área de segurança. Por outro lado, apesar de o monitor

não necessariamente precisar fazer parte do GRIS-UFRJ, o docente terá alunos com altos índices de interesse pela área a ser lecionada. Adicionalmente é bastante viável que se tenha mais de um monitor para a disciplina, dada a quantidade regular dos alunos membros do GRIS-URJ semestralmente.

4.5 Carga horária e cronograma

A carga horaria de 60 horas está de acordo com a quantidade de horas estipulada para uma disciplina optativa oferecida pelo DCC-UFRJ. A quantidade de horas reservadas para as atividades de laboratórios são maiores que as das aulas teóricas, e vão de encontro ao o projeto de tornar a disciplina bastante prática. Vale ressaltar que este cronograma é somente um escopo inicial, podendo sofrer as devidas alterações na medida que o docente responsável pela disciplina achar necessário e válido.

4.6 Pré-requisitos

O conteúdo dos livros sugeridos como referências requer diversos conceitos prévios para o bom entendimento do tema. A maioria deles já são detalhados ao longo do curso de Ciência da Computação em seus primeiros períodos. Contudo, a sugestão de Computadores e Programação (MAB353) como pré-requisito é extramente válida na medida que linguagem de máquina e Engenharia Reversa são tópicos essenciais para o entendimento de uma Análise de Malware.

4.7 Critérios de avaliação

Os critérios de avaliação sugeridos são altamente aplicáveis dentro de uma disciplina no curso de Ciência da Computação do DCC-UFRJ. Algumas outras disciplinas optativas já utilizam trabalhos práticos para avaliação de absorção do conteúdo e tais critérios não trariam nenhum empecilho para a inclusão da disciplina na grade curricular (referencia29).

4.8 Desfecho e trabalhos futuros

Foram apresentados neste trabalho diversos conteúdos que ajudariam na elaboração de uma disciplina eletiva de Segurança da Informação dentro do curso de graduação de Bacharel em Ciência da Computação do DCC-UFRJ. As avaliações feitas sobre a proposta mostram que a inclusão de uma disciplina sobre Análise de *Malware* é aplicável dentro do departamento. Trabalhos futuros para o curso de Bacharel em Ciência da Computaçã consistem em (i) fazer sua própria avaliação sobre a aplicabilidade da inserção da disciplina sugerida na grade curricular do curso; e eventualmente (ii) encontrar docentes que estariam interessados e dispostos a assumir tal projeto. Trabalhos futuros para os membros do GRIS-UFRJ podem envolver, caso o professor responsável permita e acredite ser válida a aproximação com tais alunos, (i) auxiliar na elaboração dos *slides*; (ii) auxiliar na elaboração das atividades práticas a serem feitas nos laboratórios; (iii) auxiliar na elaboração do Trabalho Final, (iv) e marcar treinamentos internos para se prepararem no auxilío aos estudantes e ao professor ao decorrer do curso.

Referências

[4:cast, 2013] - 4:cast. "Forensic 4:cast Awards 2013 Results", 2013. Disponível em https://forensic4cast.com/forensic-4cast-awards/2013-results/ Acesso em 20 de Novembro de 2016.

[AGUIAR, 2016] - Aguiar, Paulo. "AB353 2016-2 Computadores e Programação". Núcleo de Computação Eletrônica UFRJ, 2016. Disponível em: http://www.voip.nce.ufrj.br/cursos/index.php?option=com_content&view=category&id=65:mab353-2016-2-computadores-e-programacao&Itemid=62&layout=default Acesso em 15 de Dezembro de 2016.

[ARANHA, 2015] - Aranha, Diego. "MC931/MO834 - Secure Programming and Malware Analysis". Instituto de Computação Universidade de Campinas, 2015. Disponível em: https://docs.google.com/spreadsheets/d/10Wsz6pzZwOyWJaxKa8v5HGYQwiUss3C-UU_xEx1V6W8/pubhtml Acesso em: 15 de Dezembro de 2016

[BONEH; MITCHEL, 2016] - Boneh, Dan; Mitchel, John. "CS155: Computer and Network Security (Spring 2016)". Applied Cryptography Group, 2016. Disponível em: https://crypto.stanford.edu/cs155/ Acesso em: 15 de Dezembro de 2016.

[BONEH; et al., 2009] - Boneh, Dan; et al. "CS142 Web Programming and Security (Winter 2009)". Applied Cryptography Group, 2009. Disponível em: https://crypto.stanford.edu/cs142/ Acesso em: 15 de Dezembro de 2016

[CEG, 2003] - Conselho de Ensino de Graduação da Universidade Federal do Rio de Janeiro. "CEG Resolucao 02/2003". UFRJ, 2003. Disponível em http://pr1.ufrj.br/images/stories/_pr1/dmdocuments/ceg02_03.pdf Acesso em 6 de Dezembro de 2016.

[CERT, 2016] - CERT Division. "CSIRT Services". Software Engineering Institute, Carnegie Mellon University, 2016. Disponível em http://www.cert.org/incident-management/services.cfm?#ahandling Acesso em 20 de Novembro de 2016.

[CERT.BR FAQ, 2016] - CERT.br. "FAQ: Perguntas Freqüentes ao CERT.br". Núcleo de Informação e Coordenação do Ponto BR, 2016. Disponível em http://www.cert.br/docs/certbr-faq.html#6 Acesso em 20 de Novembro de 2016.

[CERT.BR, 2012] - CERT.br. Cartilha de Segurança para Internet. Comitê Gestor da Internet no Brasil, 2012. Versão 4.0, capítulo 4. Disponível em http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf Acesso em 20 de Novembro de 2016.

[CONCEITO, 2011] - Conceito.de. "Conceito de Informação". Conceito.de, 2011. Disponível em: "http://conceito.de/informacao" Acesso em 15 de Dezembro de 2016.

[GRIS, 2016] - Grupo de Resposta a Incidentes de Segurança. Portal do GRIS, 2016. Disponível em http://gris.dcc.ufrj.br/ Acesso em 20 de Novembro de 2016.

[HARRIS, 2016] - Harris, Ruth; Boneh, Dan. "CS255: Introduction to Cryptography (Winter 2016)". Applied Cryptography Group, 2016. Disponível em: http://crypto.stanford.edu/~dabo/cs255/ Acesso em: 15 de Dezembro de 2016

[HOEPERS, STEDING-JESSEN, 2016] - Hoeperes, Cristine; Stedin-Jessen, Klaus. "Fundamentos de Segurança da Internet". Escola de Governança de Internet no Brasil, 2016. Disponível em http://www.cert.br/docs/palestras/certbr-fundamentos-egijur2016.pdf Acesso em 20 de Novembro de 2016.

[JÚPITER, 2016] - Júpiter - Sistema de Graduação. "MAC0336 - Criptografia para Segurança de Dados Criptography and Data Security". Universidade de São Paulo, 2016. Disponível em: https://uspdigital.usp.br/jupiterweb/obterDisciplina?sgldis=MAC0336&codcur=45051&codhab=1 Aceso em: 15 de Dezembro de 2016

[KAASHOEK, MORRIS, 2016] - Kaashoek, Frans; Morris, Robert. "6.858: Computer Systems Security Spring 2017". MIT CSAIL Computer Systems Security Group, 2016. Disponível em: http://css.csail.mit.edu/6.858/2017/ Acesso em: 15 de Dezembro de 2016

[KASPERSKY, 2015] - Kaspersky Lab. "Security Bulletin 2015: Evolution of Cyber Threats in the Corporate Sector", 2015. Disponível em https://securelist.com/files/2015/12/KSB_2015_business_threats.pdf Acesso em 20 de Novembro de 2016.

[KELTY, 2016] - KELTY, Christopher. "The Morris Worm". Limn, 2016. Disponível em http://limn.it/the-morris-worm/ Acesso em 20 de Novembro de 2016.

[LABRADOR, 2007] - Labrador. Grupo de Resposta a Incidentes de Segurança, 2007. Disponível em http://labrador-ids.sourceforge.net/ Acesso em 20 de Novembro de 2016.

[MARQUES, 2016] - MARQUES, Thiago. "The evolution of Brazilian Malware". Secure List, AO Kaspersky Lab, 2016. Disponível em https://securelist.com/blog/research/74325/the-evolution-of-brazilian-malware/ Acesso em 20 de Novembro de 2016.

[MEC, 2003] - Ministério da Educação Conselho Nacional de Educação Câmara de Educação Superior. "Diretrizes Curriculares dos cursos de Bacharelado em Ciência da Computação, Engenharia de Computação, Engenharia de Software e Sistemas de Informação e dos cursos de Licenciatura em Computação", Câmara de Educação Superior do Conselho Nacional de Educação, 2003. Disponível em http://www.sbc.org.br/documentos-da-sbc/send/131-curriculos-de-referencia/761-diretrizes-curriculares-consulta-publica Acesso em 20 de Novembro de 2016.

[MERCÊS, 2015] - MERCÊS, Fernando. "Subindo na Hierarquia O Submundo Cibercriminoso Brasileiro em 2015". TrendLabs, 2015. Disponível em http://www.trendmicro.com.br/cloud-content/br/pdfs/business/submundo-cibercrime-brasil-2015.pdf Acesso em 20 de Novembro de 2016.

[NIST, 2012] - National Institute of Standards and Technology. "Computer Security Incident Handling Guide - Recommendations of the National Institute of Standards and Technology". U.S. Department of Commerce, 2012. Disponível em http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf Acesso em 6 de Dezembro de 2016

[PERRIG, 2016] - Perrig, Adrian. "18-487: Introduction to Computer & Network Security and Applied Cryptography". College of Engineering Carnegie Mellon University. Disponível em: https://users.ece.cmu.edu/~adrian/487-s06/487.html Acesso em: 15 de Dezembro de 2016

[QS, 2016] - QS Top Universities.com . "Top Computer Science Schools in 2016". QS Top Universities, 2016. Disponível em: http://www.topuniversities.com/university-rankings-articles/university-subject-rankings/top-computer-science-schools-2016 Acesso em: 15 de Dezembro de 2016

[RIVEST, 2016] - Rivest, RON. "6.857: Computer and Network Security (Spring 2016)". MIT CSAIL Computer Systems Security Group, 2016. Disponível em: http://courses.csail.mit.edu/6.857/2016/info Acesso em: 15 de Dezembro de 2016

[SADEH, 2016] - Sadeh, Norman. "Information Security and Privacy". School of Computer Science Carnegie Mellon University, 2016. Disponível em:

[SANTOS, 2013] - Santos, Rafael O. "Segurança em Códigos QR", Grupo de Resposta a Incidentes de Segurança, 2013. Disponível em https://drive.google.com/file/d/0B1SbSfY8fOrzSHI3UjVGNXRZUVU/view Acesso em 20 de Novembro 2016.

[SBC, 2005] - Sociedade Brasileira de Computação. "Currículo de Referência da SBC para Cursos de Graduação em Bacharelado em Ciência da Computação e Engenharia de Computação", Assembleia Geral da SBC, 2005. Disponível em http://www.sbc.org.br/documentos-da-sbc/send/131-curriculos-de-referencia/760-curriculo-de-referencia-cc-ec-versao2005 Acesso em 20 de Novembro de 2016.

[SBC, 2016] - Sociedade Brasileira de Computação. "Sobre a SBC", 2016. Disponível em http://www.sbc.org.br/institucional-3/sobre Acesso em 20 de Novembro de 2016.

[SCHNEIER, 2010] - SCHNEIER, Bruce. "The Story Behind The Stuxnet Virus". Forbes, 2010. Disponível em http://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html Acesso em 20 de Novembro de 2016.

[SIGA, 2016] - Sistema Integrado de Gestão Acadêmica. "Curso de Graduação em Bacharelado em Ciência da Computação. Curriculo a ser cumprido pelos alunos de 2010/1 a 9999/9", Departamento de Ciência da Computação, 2016. Disponível em https://siga.ufrj.br/sira/temas/zire/frameConsultas.jsp?mainPage=/repositorio-curriculo/FA9F18A7-92A4-F79B-1A98-293E97D8939B.html Acesso em 20 de Novembro de 2016.

[SIKORSKI, HONIG, 2012] - SIKORSKI, Michael; HONIG, Andrew. Practical Malware Analysis The Hands-On Guide To Dissecting Malicious Software. No Starch Press, 2012. Introduction xxviii.

[SILVA, 2016] - Silva, Anderson. "INF 1416 – Segurança da Informação". Departamento de Informática PUC-RJ, 2016. Disponível em http://www.inf.puc-rio.br/~inf1416/ Acesso em: 15 de Dezembro de 2016

[UNUCHECK, et al., 2016] - Unucheck, Roman; et al. "IT threat evolution in Q2 2016. Statistics". Kaspersky Lab, 2016. Disponível em https://securelist.com/analysis/quarterly-malware-reports/75640/it-threat-evolution-in-q2-2016-statistics/ Acesso em 20 de Novembro de 2016.

[W3SCHOOLS, 2016] - W3Schools The World's Largest Web Developer Site. "OS Platform Statistics", 2016. Disponível em http://www.w3schools.com/browsers/browsers_os.asp Acesso em 20 de Novembro de 2016.

[WORKSHOP GRIS, 2016] - Grupo de Resposta a Incidentes de Segurança. "IX Worskhop GRIS", 2016. Disponível em https://www.facebook.com/grisdccufrj/posts/1250319278329461:0 Acesso em 20 de Novembro de 2016.
http://www.normsadeh.com/isp-content Acesso em: 15 de Dezembro de 2016

Apêndice A

Exemplo de *slides* para aulas teóricas

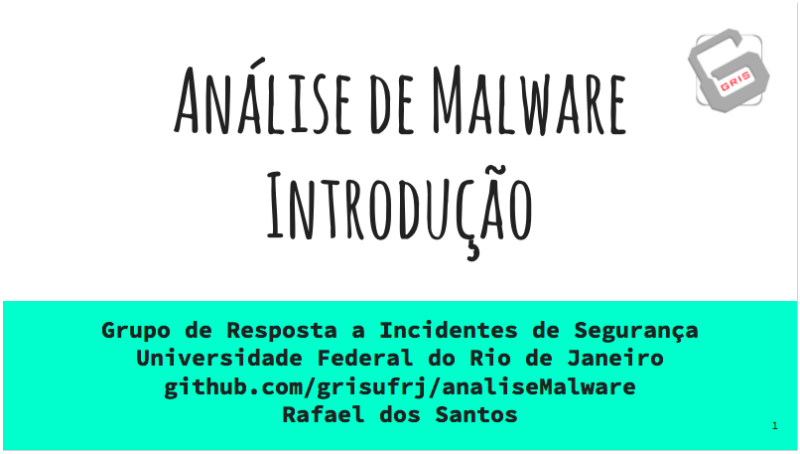

Figura A.1: *Slide* 1 - Exemplo de Aula Teórica sobre Análise de Malware

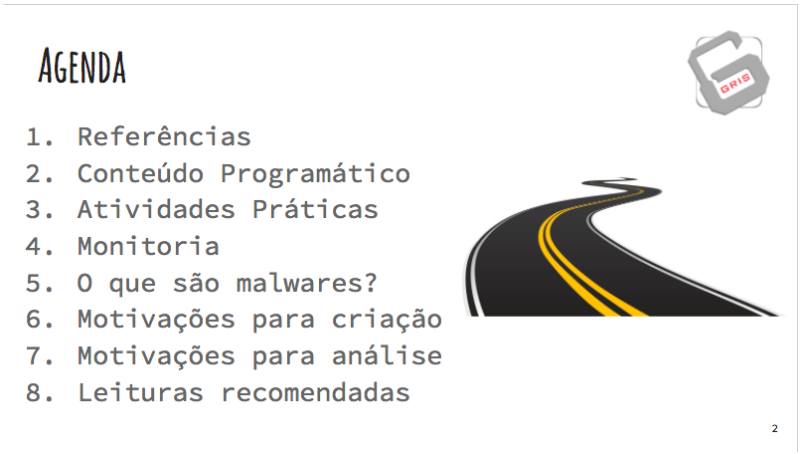

Figura A.2: *Slide* 2 - Exemplo de Aula Teórica sobre Análise de Malware

Figura A.3: *Slide* 3 - Exemplo de Aula Teórica sobre Análise de Malware

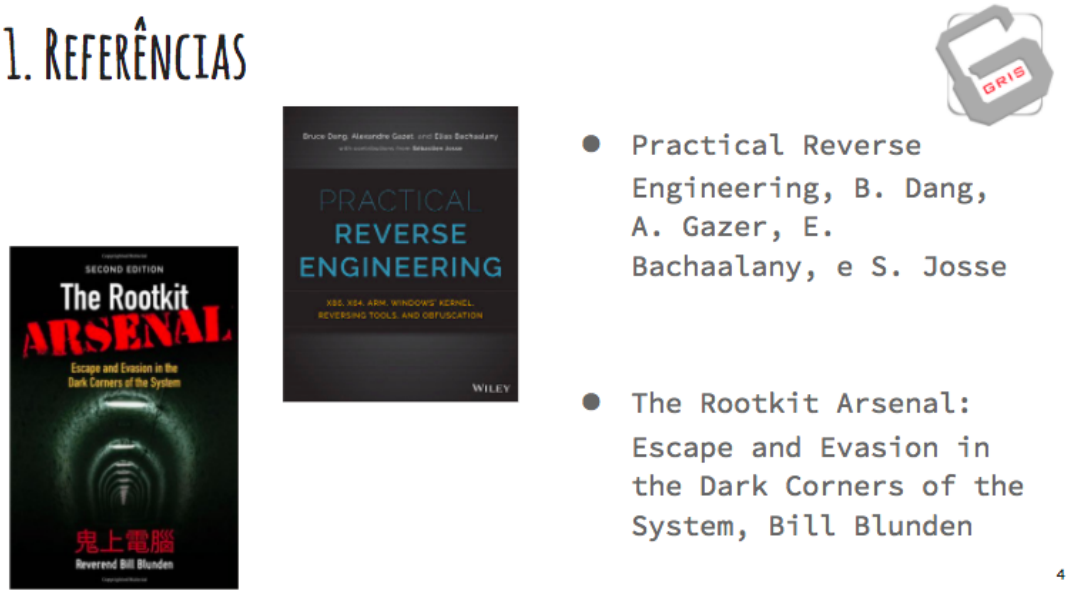

Figura A.4: *Slide* 4 - Exemplo de Aula Teórica sobre Análise de Malware

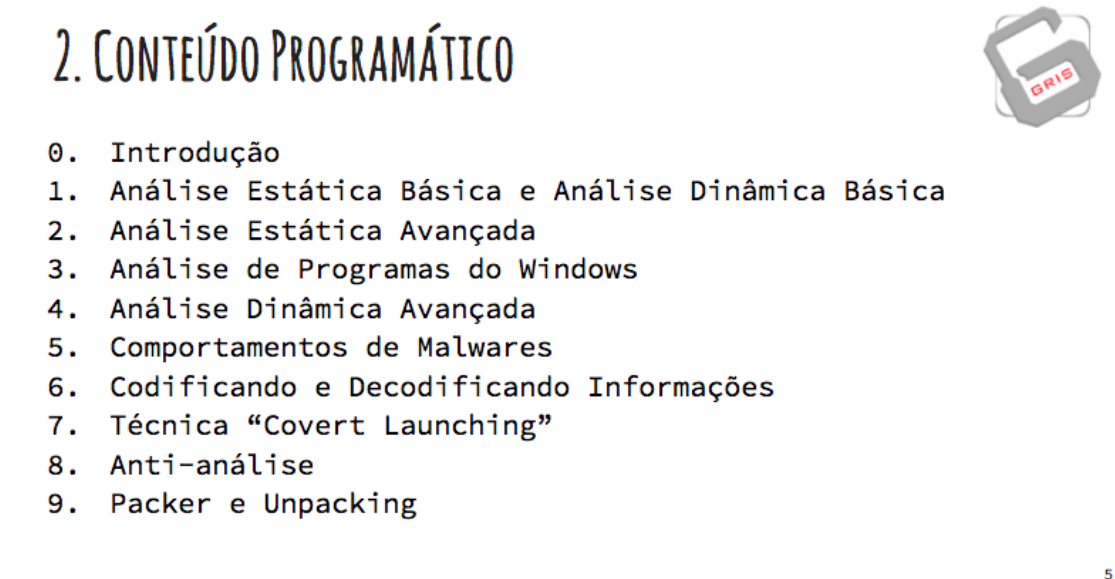

Figura A.5: *Slide* 5 - Exemplo de Aula Teórica sobre Análise de Malware

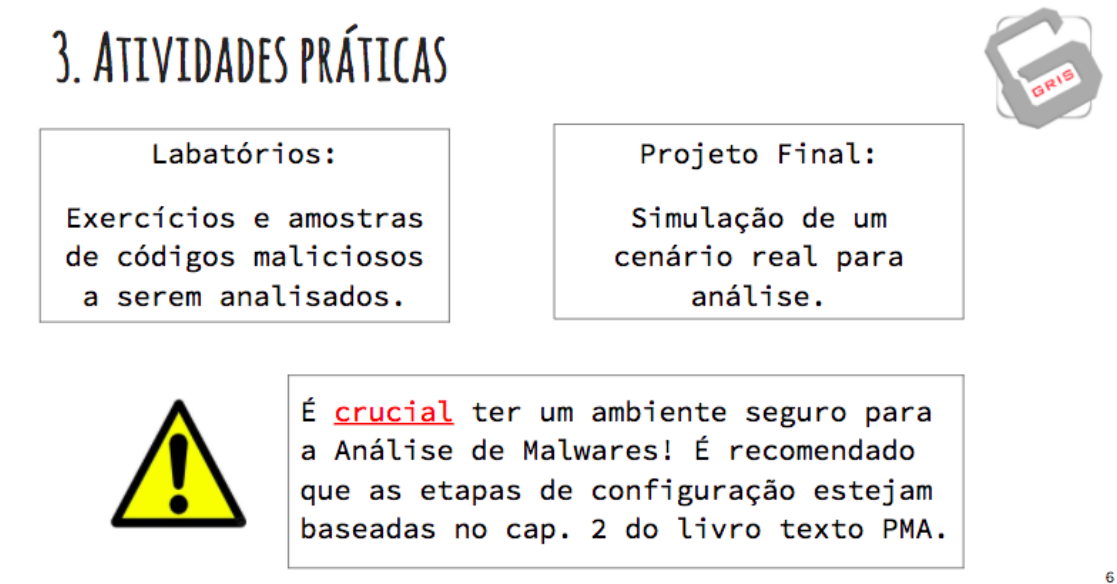

Figura A.6: *Slide* 6 - Exemplo de Aula Teórica sobre Análise de Malware

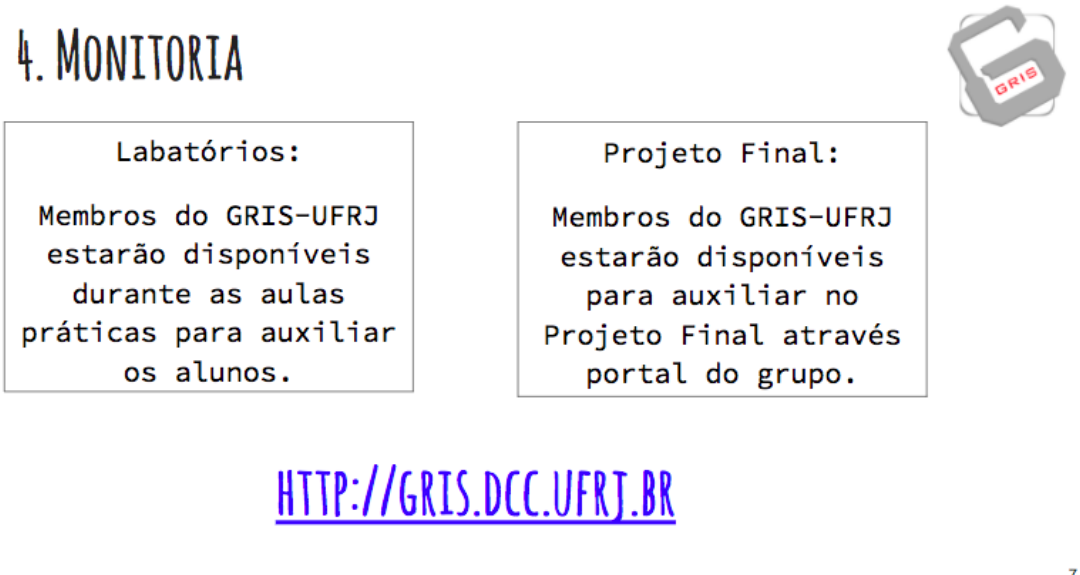

Figura A.7: *Slide* 7 - Exemplo de Aula Teórica sobre Análise de Malware

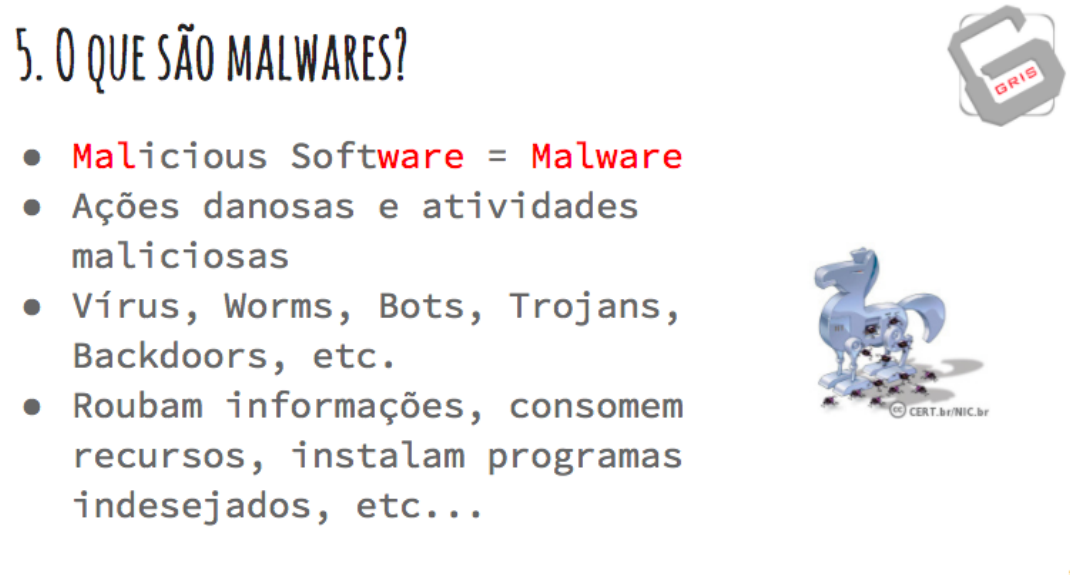

Figura A.8: *Slide* 8 - Exemplo de Aula Teórica sobre Análise de Malware

6. Motivações para criação

- Acidentalmente
- $$$$$ (na maioria dos casos)
- Guerras entre nações
- Roubo de informações

9

Figura A.9: *Slide* 9 - Exemplo de Aula Teórica sobre Análise de Malware

6. Motivações para análise

- Detecção e Respostas rápidas!
  - Remoção de ameaças
  - Análise de ameaças
  - Prevenção de ameaças
- Pesquisa
- Tornar a Internet mais segura!

10

Figura A.10: *Slide* 10 - Exemplo de Aula Teórica sobre Análise de Malware

7. Leituras recomendadas

- Cartilha CERT.br - http://cartilha.cert.br/malware/
- The Morris Worm - http://limn.it/the-morris-worm/
- Practical Malware Analysis - Intro
- Practical Malware Analysis - Cap. 0

11

Figura A.11: *Slide* 11 - Exemplo de Aula Teórica sobre Análise de Malware

Apêndice B

Programa da Disciplina

Universidade Federal do Rio de Janeiro
Centro de Ciências Matemáticas e da Natureza
INSTITUTO DE MATEMÁTICA
Departamento de Ciência da Computação

DISCIPLINA: ANÁLISE DE MALWARE (CC)

CÓDIGO: **CRÉDITOS: 4,0** **CARGA HORÁRIA: 60**
TEÓRICA: 20
PRÁTICA: 40

PRÉ-REQUISITOS:
MAB353 Computadores e Programação (CC)

PROGRAMA DA DISCIPLINA

EMENTA:
Análise Estática Básica, Análise Dinâmica Básica. Análise Estática Avançada. Análise de Programas do Windows. Análise Dinâmica Avançada e Debugging. Comportamentos de Malwares. Codificando e Decodificando informações. Técnica Covert Launching. Anti-análise. Packer e Unpacking.

OBJETIVOS GERAIS:
Capacitar o aluno adiquirá um conhecimento aprofundado sobre os formatos executáveis, Windows Internals, assim como a (API) do Windows; será capaz de extrair informações relevantes de um host e indicadores de rede que estejam eventualmente associado a um programa malicioso; conseguirá aplicar as técnicas e conceitos sobre unpack, extrair, descriptografar, ou contornar novas técnicas de anti-análise nas futuras amostras de malwares, e alcançará proficiência em ferramentas como IDA Pro, OllyDbg, WinDBG, PE Explorer, ProcMon, entre outras.

CONTEÚDO PROGRAMÁTICO:

UNIDADE I - Análise Estática Básica, Análise Dinâmica Básica
Definições sobre malwares.
Motivações para desenvolver um código malicioso.
Histórico dos malwares.
Definições sobre Análise de Malware.
Técnicas para a Análise Estática Básica.
Como configurar um ambiente seguro para análise.
Técnicas para a Análise Dinâmica Básica.

UNIDADE II – Análise Estática Avançada
Níveis de abstrações das linguagens de programação.
Definições sobre Engenharia Reversa.
Instruções, Operandos, Registradores, e Flags (x86).
Definições sobre a ferramenta IDA Pro.
Interface, Navegação, Pesquisando, Gráficos, e Plugins do IDA Pro.
Analisando códigos em C no IDA Pro.

UNIDADE III – Análise de Programas do Windows
API do Windows.

Registros do Windows. APIs de Rede. Definições sobre Dynamic Link Library (DLL). Processos, Threads, Serviços, Microsoft Component Object Model (COM). Exceptions.
UNIDADE IV – Análise Dinâmica Avançada e Debugging Definições sobre o debugging. Diferentes técnicas de debug. Definições sobre Breakpoints e Exceptions. Modificando execução de um programa com um debugger. Definições sobre as ferramentas WinDbg e OllyDbg.
UNIDADE V – Comportamentos de Malwares Downloaders e Launchers. Backdoors. Credential Stealers Mecanismos de persistência. Escalação de privilégios.
UNIDADE VI – Codificando e Decodificando informações Objetivos de analisar algoritmos de codificação. Cifras Simples. Algoritmos comuns de Criptografia. Esquemas de codificação customizáveis. Técnicas para a decodificação.
UNIDADE VII – Técnica Covert Launching Definições sobre Launchers. Injeção de processos. Substituição de processos. Injeções Hook. Injeções Asynchronous Procedure Call (APC).
UNIDADE VIII – Anti-análise Anti-Dissassembly. Anti-Debugging. Anti-Máquina Virtual. Anti-Antivírus.
UNIDADE IX – Packer e Unpacking Anatomia de um packer. Identificando programas packed. Unpacking automatizado. Unpacking manual. Packers mais comuns.

BIBLIOGRAFIA

Livro Texto:

[1] Michael Sikorski e Andrew Honig, "Practical Malware Analysis – The Hands-On Guide T\to Dissecting Malicious Software", no startch press, 2012.

Livro Complementares:

[2] Michael Ligh, Steven Adair, Blake Hartstein, e Matthew Richard, "Malware Analyst's Cookbook", Wiley Publishing, 2010.

[3] Bruce Dang, Alexandre Gazet, Elias Bachaalany, e Sébastien Josse, "Practical Reverse Engineering", Wiley Publishing, 2014.

[4] Bill Blunden, "The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System", Paperback, 2 edição, 2009.

CRITÉRIO DE AVALIAÇÃO:

Trabalhos práticos

APLICATIVO(S) NECESSÁRIO(S):

IDA Pro, OllyDbg, WinDBG, PE Explorer, ProcMon, Kali Linux