MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA
INSTITUTO MILITAR DE ENGENHARIA
CURSO DE MESTRADO EM SISTEMAS E COMPUTAÇÃO

REGIS DE SOUZA DE CARVALHO

PROPOSTA DE ARQUITETURA PARA COLETA DE ATAQUES CIBERNÉTICOS ÀS INFRAESTRUTURAS CRÍTICAS

Rio de Janeiro
2014

INSTITUTO MILITAR DE ENGENHARIA

REGIS DE SOUZA DE CARVALHO

PROPOSTA DE ARQUITETURA PARA COLETA DE ATAQUES CIBERNÉTICOS ÀS INFRAESTRUTURAS CRÍTICAS

Dissertação de Mestrado apresentada ao Curso de Mestrado em Sistemas e Computação do Instituto Militar de Engenharia, como requisito parcial para obtenção do título de Mestre em Sistemas e Computação.

Orientadores: Prof. Anderson F. P dos Santos - D.Sc
Prof. Antonio E. Carrilho da Cunha - D.Sc

Rio de Janeiro
2014

INSTITUTO MILITAR DE ENGENHARIA

Praça General Tibúrcio, 80 – Praia Vermelha

Rio de Janeiro – RJ CEP: 22290-270

005.8 Carvalho, Regis de Souza de

C331p Proposta de arquitetura para coleta de ataques cibernéticos às infraestruturas críticas / Regis de Souza de Carvalho, orientado por Santos, Anderson F.P. Dos e Cunha, Antonio E. Carrilho da – Rio de Janeiro: Instituto Militar de Engenharia, 2014.

57p. : il

Dissertação (mestrado) – Instituto Militar de Engenharia, Rio de Janeiro, 2014.

1. Curso de Sistemas e Computação – teses e dissertações. 2. Cibernética. 3. Redes de Computadores – medidas de segurança I. Santos, Anderson F.P. dos. II. Cunha, Antonio E. Carrilho da III. Título. IV. Instituto Militar de Engenharia.

INSTITUTO MILITAR DE ENGENHARIA

REGIS DE SOUZA DE CARVALHO

PROPOSTA DE ARQUITETURA PARA COLETA DE ATAQUES CIBERNÉTICOS ÀS INFRAESTRUTURAS CRÍTICAS

Dissertação de Mestrado apresentada ao Curso de Mestrado em Sistemas e Computação do Instituto Militar de Engenharia, como requisito parcial para obtenção do título de Mestre em Sistemas e Computação.

Orientadores: Prof. Anderson Fernandes Pereira dos Santos - D.Sc
Prof. Antonio Eduardo Carrilho da Cunha – D.Sc

Aprovada em 26 de setembro de 2014 pela seguinte Banca Examinadora:

_____
Prof. Anderson Fernandes Pereira dos Santos - D.Sc. do IME - Presidente

_____
Prof. Antonio Eduardo Carrilho da Cunha – D.Sc. do IME

_____
Prof. Oumar Diene – D.Sc da UFRJ

_____
Profª. Raquel Coelho Gomes Pinto – D.Sc do IME

Rio de Janeiro
2014

"Para realizar grandes conquistas, devemos não apenas agir, mas também sonhar; não apenas planejar, mas também acreditar”. (Anatole France)

AGRADECIMENTOS

Agradeço inicialmente a Deus, pois sem ele nada seria possível.

A todos os professores e funcionários do curso de mestrado em Sistemas e Computação - SE/8, em especial aos professores orientadores, pelo apoio na orientação deste trabalho.

Aos professores da banca por aceitarem participar da avaliação deste trabalho.

Ao Laboratório de Monitoramento de Processos do curso de Engenharia Nuclear da COPPE/UFRJ pelo apoio na cessão do laboratório para a produção dos testes realizados neste trabalho.

A Eletrobras Eletronuclear S.A pela cessão de equipamentos e minha disponibilidade em período parcial, para a realização deste curso e concretização deste objetivo.

A minha família, em especial à minha esposa, pelo apoio incondicional.

Regis de Souza de Carvalho

SUMÁRIO

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS

ANOVA	-	Análise da variância
API	-	Interface de Programação de Aplicativos
CLP	-	Controlador Lógico Programável
DSIC	-	Depto.de Segurança da Informação e Comunicações
DoS	-	*Deny of Service*
DDoS	-	*Distributed Deny of Service*
ES-ISAC	-	Centro de Análise e Informações do Setor Elétrico
GSI/PR	-	Gabinete de Segurança Institucional da Presidência
HMI	-	Interface Homem Máquina
HTTP	-	*Hyper Text Transfer Protocol*
IPS	-	Sistema de Prevenção a Intrusão
SCADA	-	Sistema de Controle e Aquisição de Dados
SMB	-	*Service Message Block*

RESUMO

A Defesa Cibernética das infraestruturas críticas nacionais tornou-se um importante desafio, principalmente diante do atual cenário de ataques cibernéticos aos diversos países, com o surgimento de diversos *malwares* atacantes de ativos críticos de instituições estratégicas para a segurança e soberania nacional. *Honeypots* são sensores baseados em anomalias, sendo considerados como ferramentas importantes na detecção de ataques cibernéticos, para a mitigação dos riscos e ameaças às infraestruturas críticas. A utilização de *honeypots* simulando os ativos críticos alvos das ameaças cibernéticas se faz necessária para identificação real dos ataques e ameaças existentes.

Este trabalho propõe uma arquitetura denominada *honeySCADA* que coleta ataques cibernéticos direcionados aos sistemas industriais SCADA, através da simulação da interação entre um equipamento do operador do sistema SCADA com um *honeypot* que simula um CLP (controlador lógico programável), ativo importante do sistema SCADA, na rede de uma empresa da infraestrutura crítica nacional.

Foi realizada a avaliação do *honeySCADA* proposto analisando a sua similaridade através de uma avaliação estatística do serviço Modbus IP, que se faz essencial para o funcionamento destes ativos em redes de produção industrial. Com base na arquitetura proposta e a identificação dos diversos ataques recebidos, faz-se uma comparação com trabalhos recentes, resultando em maiores quantidades de ataques específicos ao equipamento do operador e ao *honeyCLP.* É realizada uma simulação de ataque explorando vulnerabilidades do equipamento do operador, exploradas no ataque Stuxnet, sendo coletados os ataques semelhantes recebidos pela arquitetura para comparação, contribuindo para as pesquisas existentes no âmbito da defesa cibernética nas infraestruturas críticas.

ABSTRACT

The Cyber Defense of national critical infrastructure has become an important challenge, principally given the current scenario of cyber attacks on several countries, with the emergence of various malware attackers of critical assets of strategic institutions for security and national sovereignty. Honeypots are sensors based on anomalies, considered as important tools on detections of cyber attacks, to mitigate the risks and threats on these critical infrastructure. The use of honeypots simulating the targets of cyber threats critical assets is necessary to identify real attacks and existing threats. This work proposes an architecture called honeySCADA for collect cyber attacks targeted at industrial SCADA systems, by simulating the interaction between an equipment operator's SCADA system with a honeypot that simulates a PLC (programmable logic controller) active major SCADA system in a business network of the national critical infrastructure. Evaluating the proposed honeySCADA was performed by analyzing the similarity of a statistical evaluation of the Modbus IP service, which becomes essential for the functionality of these industrial network. Based on the proposed architecture and the identification of several attacks received, makes a comparison with recent work, resulting in greater amounts of specific attacks targeting the equipment of the operator and the honeyCLP. Simulating the attack exploiting vulnerabilities of the equipment operator, explored on the Stuxnet attack, being collected similar attacks received by the architecture for comparison, contributing to existing research within the critical infrastructure cyber defense.

1 INTRODUÇÃO

Nos últimos anos, com a evolução tecnológica mundial, surgiram inovações fundamentais na área da computação (DE MATTOS e GUIMARÃES, 2005) como a automatização dos dados através das redes de computadores. O cenário tecnológico atual proporciona trocas de informações entre pessoas e instituições, gerando um ambiente de interação mundial. Este ambiente se chama espaço cibernético.

Infraestruturas críticas são instalações, bens e ativos que possuem serviços que, se interrompidos, provocam sérios impactos sociais, econômicos e políticos (BRANQUINHO et al., 2014).

Infraestruturas críticas também são definidas como os ativos que se afetados por fenômenos da natureza, como terremotos, inundações ou por ações de terrorismo, causam grandes impactos em toda uma nação e sua sociedade (CANONGIA, 2009). São definidas também como os subconjuntos de ativos que afetam a continuidade da missão do Estado e a segurança da sociedade (MANDARINO, 2010).

Diversas ameaças cibernéticas direcionadas às infraestruturas críticas de diversos países surgiram nos últimos anos, demonstrando a necessidade de desenvolvimento de técnicas de defesa, no intuito da manutenção da segurança nacional destes países.

Neste trabalho é proposta uma arquitetura *honeySCADA,* simulando a interação entre um operador deste sistema industrial com um CLP[1] Siemens S7, o qual é simulado através do *honeyCLP*.

A similaridade do CLP Siemens com o *honeyCLP* é comparada através da *utilização dos* métodos estatísticos ANOVA e TESTE T Student, aplicados aos tráfegos de dados coletados a partir da utilização da ferramenta PLCSCAN com o CLP real e com o *honeyCLP*.

[1]CLP's: Controladores Lógico-Programáveis

É realizada uma simulação de ataque semelhante ao Stuxnet, direcionado ao equipamento do operador, para análise e comparação com os ataques recebidos da INTERNET.

Esta arquitetura tem o objetivo de coletar os ataques cibernéticos direcionados às infraestruturas críticas industriais.

1.1 MOTIVAÇÃO

Honeypots são simuladores de serviços de redes que, em conjunto com outras ferramentas, ajudam nas detecções de ataques. Eles simulam serviços de rede com o objetivo de atrair conexões suspeitas (TJELTA, 2011).

Os diversos ataques citados na seção 2.3.2 deste trabalho, oriundos de ameaças direcionadas às infraestruturas críticas, demonstram a necessidade de ações proativas na segurança cibernética destas infraestruturas críticas.

Face ao exposto, são motivações para este trabalho os seguintes fatores:

- O crescimento do número de ataques cibernéticos às infraestruturas críticas do setor elétrico mundial;
- Necessidade de sensores de detecção de ataques às redes industriais, no âmbito das infraestruturas críticas.

1.2 OBJETIVOS

1.2.1 OBJETIVO PRINCIPAL

O principal objetivo deste trabalho é propor uma arquitetura *honeySCADA*, composta por um operador interagindo com o *honeyCLP, que* simula um CLP real Siemens S7, para coletar dados de ameaças de ataques cibernéticos direcionados às redes de sistemas industriais SCADA.

1.2.2 OBJETIVOS ESPECÍFICOS

Para atingir o objetivo proposto é necessário:

- A validação da similaridade entre o *honeyCLP* e o CLP Siemens S7, para composição do *honeySCADA*;

- A validação do uso em produção do *honeySCADA* proposto.

1.3 ORGANIZAÇÃO DA DISSERTAÇÃO

Além da introdução, este trabalho contém ainda cinco capítulos, cada um abrangendo os seguintes assuntos:

- O **Capítulo 2** é dedicado aos conceitos básicos de infraestruturas críticas, contendo alguns setores estratégicos e críticos para a segurança nacional, incluindo-se os sistemas de controle e aquisição de dados – SCADA. Apresenta também os principais conceitos envolvendo a segurança nas infraestruturas críticas, contendo uma introdução neste assunto, descrevendo os ataques ocorridos recentemente em âmbito internacional;

- O **Capítulo 3** apresenta em detalhes a arquitetura *HoneySCADA* proposta por este trabalho, seus componentes, validação por experimentos, análise dos ataques recebidos e trabalhos relacionados;

- Finalmente, o **Capítulo 4** descreve as considerações finais a respeito dos trabalhos e pesquisas desenvolvidos, citando a conclusão e recomendações para trabalhos futuros.

2 INFRAESTRUTURAS CRÍTICAS

2.1 INTRODUÇÃO

Infraestruturas críticas são aquelas que se afetadas por fenômenos da natureza, como terremotos, inundações ou por ações de terrorismo, causam grandes impactos em toda uma nação e sua sociedade.

São exemplos de infraestruturas críticas: os sistemas de telecomunicações, os sistemas de transporte, os de distribuição de água e as geradoras e distribuidoras de energia (CANONGIA, 2009).

As infraestruturas críticas exercem forte influência no cotidiano das pessoas e na operação de setores importantes para o desenvolvimento, manutenção e sustentabilidade de uma nação. Elas são importantes devido às facilidades e utilidades que oferecem à sociedade e, principalmente, por subsidiarem na forma de recurso ou serviço, outras infraestruturas críticas de igual ou maior nível de complexidade.

Com a evolução da integração entre as infraestruturas críticas, ocorre a dependência entre elas. Como exemplo, as indústrias de energia exercem um papel fundamental no funcionamento dos sistemas de abastecimento de água e de transportes. Como exemplo dessa interdependência, observa-se a importância das indústrias de energia, que são essenciais ao funcionamento das empresas de abastecimento de água e do setor de transportes (GHORBANY e BAGHERY, 2008).

Os ativos de informação pertencentes às infraestruturas críticas são itens fundamentais e relevantes às suas respectivas instituições, pois possuem valor estratégico e necessitam de proteções adequadas.

Além disso, as evoluções tecnológicas da computação causam dependências tecnológicas entre sistemas e serviços, como o compartilhamento de recursos, que expõe as organizações às diversas ameaças, entre elas: fraudes eletrônicas, espionagem, sabotagem, vandalismo, incêndio, inundação, blackouts, códigos maliciosos, ataques DDoS, entre outras (ABNT, 2005).

Diante do acima exposto, os ataques cibernéticos contra os serviços pertencentes a estas infraestruturas críticas e estratégicas, podem afetar diretamente a continuidade da missão do Estado e da segurança nacional, diante do

impacto que possa ser causado na interrupção destes serviços essenciais à sociedade e ao Estado.

2.1.1 SISTEMAS DE TELECOMUNICAÇÕES

Os sistemas de telecomunicações são amplamente utilizados pela sociedade global, possuindo grande relevância nos setores governamentais e empresariais de maneira geral. São infraestruturas críticas de grande importância, haja vista o impacto que podem causar, principalmente no âmbito da economia regional e global, em caso de interrupção dos seus serviços.

Como exemplo principal da sua importância, destaca-se o ataque ao complexo do *World Trade Center*, ocorrido em Nova York - EUA, na data de 11 de setembro de 2001. Como consequência, causou a interrupção de serviços críticos de telecomunicações, devido à concentração de *datacenters* e *backbones* de diversas empresas do ramo, impactando principalmente no âmbito da economia daquele país (WHITTINGTON et al., 2012).

Em (ROBERTS, 2009) é analisado o impacto deste desastre na macroeconomia do país, demonstrando uma queda de 0,5% no crescimento real do PIB e uma redução de 598 mil postos de trabalho. O desenvolvimento de centros tecnológicos empresariais com alta disponibilidade de serviços compartilhados concentrados em localidades específicas, resultam em riscos potenciais, no caso da indisponibilidade destes serviços.

A concentração de infraestruturas de telecomunicações em localizações geográficas centrais tem evoluído nos últimos anos, devido à economia nos custos de pessoal, de espaço e equipamentos compartilhados. Além disso, a diversidade de protocolos de rede aumenta a variedade de serviços que podem ser oferecidos sem aumentar os custos operacionais com a oferta destes diversos serviços.

De acordo com (PARFOMAK, 2008), estes fatores de risco têm crescido nos EUA, principalmente diante da diversidade de serviços e protocolos de redes, proporcionando cada vez mais serviços à sociedade, ampliando-se a dependência e os riscos em caso de indisponibilidade.

Em (MOSS et al.,2005) observa-se que as empresas do setor de telecomunicações que possam ser prejudicadas e ter dificuldades em resistir a um

evento catastrófico, são necessárias para estimular a recuperação da economia na sequência de um desastre. Isto se dá pela interdependência com infraestruturas de outros setores, onde os danos em telecomunicações possam impactar outros setores críticos, como sistemas elétricos, de transporte e setor bancário, causando impactos econômicos e sociais.

Existe uma grande necessidade de desenvolvimento de políticas e controles governamentais, visando o estabelecimento e padronização de regras para as empresas públicas e privadas, no intuito de se obter resiliência nas infraestruturas deste setor, diante da dificuldade de mapeamento e controle dos ativos e riscos inerentes ao setor de telecomunicações.

Diante da complexidade e importância dos sistemas de telecomunicações, as diversas empresas privadas atuantes neste segmento podem não ter a capacidade de avaliação dos riscos existentes. Tal fato, seja pela falta de prioridade desta avaliação no plano estratégico dessas empresas ou pela falta de regulação do Estado, deve ser objeto de ações governamentais no estabelecimento de segurança e resiliência deste setor (VILLASENOR, 2011).

2.1.2 SISTEMAS DE TRANSPORTES

A sua aplicação se dá especificamente nos sistemas de controle de sinais de trânsito, possuindo alto nível de responsabilidade na organização da sociedade.

Como exemplo do impacto que podem ser causados em caso de falhas desses sistemas, os engarrafamentos e desorganização no sincronismo dos sinais, podem causar interrupção no fornecimento de bens de consumo à sociedade.

A dependência entre os setores de infraestruturas críticas pode gerar um efeito cascata na interrupção de serviços essenciais. Este setor depende fortemente do fornecimento estável de energia adequada para seu funcionamento, entretanto é um setor que também é provedor de outros serviços que dependem de mobilidade urbana, como o transporte de matéria

prima da indústria, do abastecimento de alimentos, além do transporte médico de pacientes emergenciais.

Em (DHS, 2011), o plano específico de segurança para o setor de transportes define uma estrutura de gestão de riscos, contendo os passos básicos para a redução dos riscos aos ativos, sistemas e redes pertencentes ao setor. É um complemento ao Plano de Parceria para Segurança e Resiliência de Infraestruturas Críticas (DHS, 2013).

2.1.3 SISTEMAS DE DISTRIBUIÇÃO DE ÁGUA

Os sistemas de distribuição de água são infraestruturas críticas que afetam diretamente a estabilidade e a qualidade de vida da população de uma sociedade. Sua importância é vital, pois tem relação direta com a saúde, sendo meio de subsistência aos cidadãos.

Em (BELLAVITA, 2012) são apresentados os possíveis impactos mundiais referentes à escassez de água a médio e longo prazo, citando estudos que analisam detalhadamente a situação do setor hídrico nos estados estratégicos dos EUA, principalmente os que se posicionam próximos às fronteiras.

Estes estudos afirmam que durante os próximos 10 anos, alguns estados dos EUA e países importantes e estratégicos terão problemas no fornecimento de água, podendo ocorrer instabilidades sociais em nível internacional.

Afirma-se que de 2012 a 2040, a disponibilidade de água doce não vai acompanhar a demanda global, sendo necessária uma gestão eficaz dos recursos hídricos mundiais. Os problemas dificultarão a capacidade dos países na produção de alimentos e geração de energia, sendo um risco aos mercados globais de alimentos e ao crescimento econômico dos países. Locais como o norte da África, o Oriente Médio e o Sul da Ásia estão em amplo desenvolvimento demográfico e econômico, estando assim entre os que enfrentarão grandes desafios no fornecimento de água.

Em (NIC, 2012) é apresentado um relatório deste setor, que possui foco na relação entre a segurança do setor hídrico e os interesses globais dos EUA. Neste relatório estão inseridos alguns aspectos importantes sobre os acordos existentes

neste setor, citando os riscos, oportunidades e questões principais como a escassez de água nos países parceiros dos EUA durante os próximos 10 anos, assim como o impacto desta escassez na produção mundial de alimentos e energia elétrica até 2040.

Neste documento é declarado que um acordo de 1944 entre os Estados Unidos e o México estipula os termos de partilha de água dos rios fronteiriços entre os dois países, com as obrigações de fornecimento de água de cada lado, onde é definido que os Estados Unidos (EUA) tem direito a receber parte dos tributos gerados pelo uso dos rios mexicanos, entretanto não havendo a reciprocidade com o México, sendo classificado como injusto por muitos.

O acesso universal à água e saneamento está contemplado em (UNICEF, 2013), que desenvolve um plano de atividade global para atingir metas de combate à pobreza em 2015.

Este projeto é essencial, pois estudos identificaram que em média, uma criança morre de uma doença relacionada com a água a cada 15 segundos, e a água não potável e falta de saneamento são as principais causas de morte no mundo, para crianças menores de cinco anos de idade. Além disso, metade de todas as pessoas que vivem nas nações em desenvolvimento está sofrendo de um problema de saúde relacionado com déficits de água e saneamento (UNICEF, 2013).

O (NIC, 2012) confirma que a experiência dos EUA em gestão de recursos hídricos nos setores público e privado é altamente considerada. Diante dos futuros problemas da escassez, certamente serão procurados por todos os países para liderar a comunidade global no desenvolvimento e implementação de políticas de gestão de recursos hídricos mundiais.

A falta de água adequada será um fator de desestabilização em alguns países porque eles não têm recursos financeiros ou capacidade técnica para resolver esses problemas. A falta destes recursos foi citada por pesquisadores como um fator de conflito político e até mesmo de guerra. Entretanto a água poderá servir como um ponto de entrada potencial para a paz mundial e apoio na cooperação sustentável entre as nações.

No Brasil existem projetos no âmbito da ANA (Agência Nacional de Águas) que disponibilizam informações em tempo real sobre as bacias hidrográficas do país. O Sistema Brasileiro Hidrológico e o Sistema de Monitoramento Hidrológico no Setor

Elétrico são exemplos destes sistemas, que fornecem dados essenciais para a gestão dos recursos hídricos nacionais (ANA, 2010).

2.1.4 SISTEMAS DE ENERGIA ELÉTRICA

Os sistemas de energia elétrica, que são compostos por empresas de geração e distribuição de energia elétrica são infraestruturas críticas, semelhantes aos sistemas de telecomunicações, e que sustentam outros setores críticos. Como exemplos desse setor, as usinas nacionais de geração de energia elétrica mais comumente utilizadas nacionalmente são as hidrelétricas (movidas à água) e térmicas (movidas a gás, a carvão e fusão nuclear).

A energia elétrica proporciona atualmente diversos recursos essenciais para o funcionamento de uma sociedade, sendo vital para as pessoas em seu dia a dia. O crescimento natural do consumo de energia pela sociedade gera a necessidade de um amplo planejamento no âmbito governamental, visando a alta disponibilidade do sistema através de implementações de infraestruturas resilientes e capazes de suportar eventuais falhas.

Em (DHS, 2011), o plano de segurança de infraestruturas críticas nacionais do setor elétrico reafirma a importância desse setor, afirmando que sem um fornecimento estável de energia, a saúde e bem-estar da população são ameaçados, causando instabilidade na economia dos EUA. Mais de 80% da infraestrutura de energia do país é de propriedade do setor privado, fornecendo para o setor de transportes, para as residências, empresas e outras fontes de energia que são essenciais para o crescimento e produção de todo o país.

Considerando–se a importância deste setor como recurso fundamental para a estabilidade e funcionamento dos demais setores de infraestruturas críticas, cabe ao governo promover ações sistemáticas e contínuas junto ao setor privado, resultando em estudos para análise dos impactos de ameaças existentes e desenvolvendo ferramentas e tecnologias no intuito de evitar e limitar as consequências das ações destas ameaças.

Há evidências que os grandes apagões ocorridos nos últimos anos são muitas vezes causados por uma concorrência de eventos, que incluem defeitos nos componentes elétricos dos sistemas de controle, erros humanos de operadores, e mau funcionamento no sistema de telecomunicações, fato este que evidencia a integração entre setores distintos das infraestruturas críticas (BECCUTI, 2012).

Diante da necessidade de ações conjuntas de todas as esferas governamentais, foi criado nos EUA um Conselho de Governo para Coordenação do setor de Energia no ano de 2004, e representando as organizações federais relacionadas com a energia, bem como os governos estaduais e locais e designando grupos de trabalho conjuntos que permanecem trabalhando juntos para proteger infraestrutura crítica de energia dos EUA (DHS, 2011).

No Brasil foi criado no ano 2000 o CGSI - Comitê Gestor da Segurança da Informação, subordinado ao Departamento de Segurança da Informação e comunicações e que assessora a Secretaria Executiva do Conselho de Defesa Nacional na implantação das diretrizes da Política de Segurança da Informação, nos órgãos e nas entidades da Administração Pública Federal, sendo composto por representantes dos diversos ministérios, principalmente o das Minas e Energia, que possui sob sua responsabilidade grande parte da geração de energia no âmbito do país (CDN, 2009).

Os trabalhos citados demonstram a necessidade de desenvolvimento e integração governamental, além das empresas do setor privado que estejam inseridas como infraestruturas críticas nacionais. As iniciativas existentes nos EUA demonstram a importância dessa integração em outros países, que proporciona um mapeamento dos ativos críticos e facilitando ações de contingência e mitigação dos riscos existentes ao setor, fortalecendo assim a segurança nacional.

Dos setores de infraestruturas críticas citadas neste capítulo, os itens 2.1.2 - Sistemas de Transportes, 2.1.3 - Sistemas de Distribuição de Água e 2.1.4 - Sistemas de Energia Elétrica, são os que possuem os sistemas SCADA na sua estrutura geral de funcionamento.

2.2 SISTEMAS DE CONTROLE E AQUISIÇÃO DE DADOS (SCADA)

2.2.1 DESCRIÇÃO

O Sistema SCADA é um sistema utilizado na automação e controle de dados de redes industriais, utilizado mundialmente em infraestruturas críticas industriais. Atua no controle e coleta de dados dos sensores e instrumentos localizados em locais remotos, conectados a um centro de controle para monitoramento e operação.

Este sistema foi desenvolvido em meados de 1960 para uso em redes isoladas e de arquitetura centralizada.

A partir da década de 90 com a evolução das tecnologias de redes de comunicação, estas passaram a serem adotadas como meios de comunicação dos Sistemas SCADA, utilizando uma arquitetura de amplo alcance geográfico (KANG, 2009) e (JANICKE, 2012).

2.2.2 COMPONENTES

O Sistema SCADA possui em sua composição servidores, dispositivos para comunicação e controle da sua rede industrial. Os principais componentes são os servidores de banco de dados, os servidores de aplicação, com sistemas supervisórios e aplicações para interação com o CLP (controlador lógico programável), dispositivos de campo, e os dispositivos industriais (motores, sensores, válvulas, etc.).

O CLP atua como dispositivo mestre, enviando dados e programações aos dispositivos escravos, que são sensores ou atuadores da planta industrial (IGURE et al., 2006).

Este sistema utiliza o protocolo Modbus, que atualmente é utilizado nas redes SCADA integradas com redes ethernet, sendo chamado de Modbus IP. Este Protocolo originalmente foi desenvolvido para atuação em redes isoladas sem a preocupação com a segurança, sendo necessária a sua adaptação para atuar em redes descentralizadas e heterogêneas.

As redes industriais de empresas com grande expansão territorial, utilizam esta arquitetura descentralizada e com interconectividade integrando suas redes operativas e corporativas (ZHENDONG, 2012).

2.2.3 FUNCIONAMENTO

Na estrutura de funcionamento do sistema SCADA, servidores e estações de trabalho (equipamento de operação) são utilizadas pelos operadores para interagir com os dispositivos da rede de operação. Os servidores de aplicação usados pelos operadores, atuam na rede de operação, proporcionando o controle e interpretação dos dados dos CLP's.

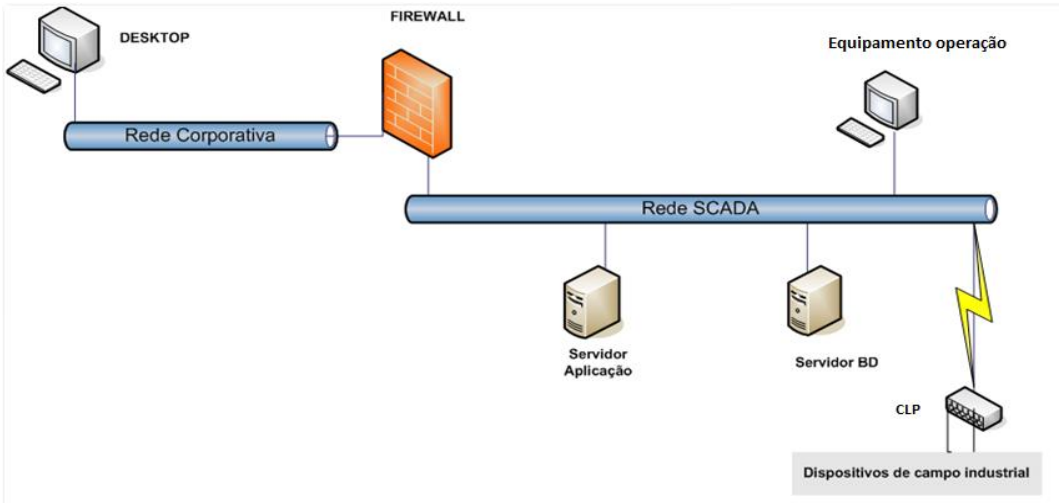

FIG. 2.1 – Arquitetura do Sistema SCADA (Adaptado de (JANICKE, 2012))

Conforme ilustrado na FIG. 2.1 a arquitetura do sistema SCADA atualmente é estruturada com interconectividades entre as redes de operação industrial e corporativa.

Na integração entre as redes SCADA e corporativa, as comunicações entre os dispositivos são realizadas através de redes ethernet (CHIKUNI et al., 2007).

Atualmente, com a expansão das redes WiFi, já há sistemas SCADA com o uso da tecnologia Wireless (KANG, 2009).

Os novos sistemas de controle industrial inevitavelmente serão baseados em serviços *web* e utilizarão a Internet como meio de comunicação (MAHBOOB et al., 2010).

O equipamento do operador pode ser considerado como o principal ativo da rede SCADA, pois é utilizado no monitoramento e administração dos CLP´s e dispositivos de campo industrial, sendo um alvo em potencial.

Esta integração traz riscos relevantes aos sistemas industriais, onde as ameaças existentes contra as redes corporativas passaram a ser também ameaças às redes industriais.

2.3 SEGURANÇA NAS INFRAESTRUTURAS CRÍTICAS

Tendo em vista a importância das instituições que compõem as infraestruturas críticas de um país para a segurança nacional, devem ser adotadas e implementadas estratégias efetivas para evitar, minimizar e mitigar os riscos oriundos das ameaças existentes.

Como estratégias internacionais no âmbito da segurança cibernética, foram identificadas ações governamentais dos EUA, como a criação de instituições específicas para atuação nesse sentido. O ES-ISAC, que é um Centro de Análise e Informações do Setor Elétrico dos EUA, foi criado em 1998 para facilitar a comunicação entre os participantes da indústria, do governo federal e de outras infraestruturas críticas.

Possui a finalidade de divulgar análises técnicas de possíveis ameaças, de forma confiável e segura, ajudando a indústria de energia a tomar medidas adequadas de proteção. Atua na gestão de incidentes como um canal de comunicação segura para o setor elétrico dos EUA, aumentando a capacidade do setor para se preparar e responder às ameaças físicas e cibernéticas.

No Brasil o DSIC – Departamento de Segurança da Informação e Comunicações, órgão subordinado ao GSI/PR – Gabinete de Segurança Institucional da Presidência da República, elabora normas que definem estrategicamente a segurança da informação nas instituições que compõem as infraestruturas críticas da administração pública federal.

Dentre suas atribuições, destaca-se a coordenação e execução de ações de segurança da informação e comunicações, definindo requisitos para a implantação da segurança nas instituições da administração pública federal. Além disso, dentre suas missões está a de promover a operacionalização e manutenção do centro de tratamento e resposta a incidentes que ocorram nas redes de computadores da administração pública federal.

Dentre as suas normas publicadas, destaca-se o Guia de Referência para a Segurança das Infraestruturas Críticas da Informação, que identifica nos requisitos mínimos necessários, o uso de sensores para detecção de ataques (DSIC, 2010).

2.3.1 VULNERABILIDADES

As vulnerabilidades existentes nas redes corporativas impactam a segurança das redes industriais, devido a interconectividade destas redes, causando ameaças à segurança dos Sistemas SCADA (KANG, 2009), (PIRES, 2006) e (JANICKE, 2012).

Os dados do sistema SCADA são acessados pelos servidores de gerenciamento de banco de dados corporativos, integrando as bases de dados com eficiência, entretanto com o risco de receberem os ataques da rede corporativa (LEE, 2010).

Em (KANG, 2009) numa análise e definição dos pontos de vulnerabilidades da rede SCADA, são identificados os mesmos ataques internos de uma rede corporativa como ameaças ao sistema SCADA.

As principais ameaças identificadas são:

- Acesso não autorizado ou violação de acesso – Nesta atividade um atacante se utiliza de ferramentas e técnicas para acessar sistemas e dados controlados, causando a quebra da segurança destes sistemas;
- *Backdoor* – Nesta ameaça o acesso remoto ao computador da vítima ocorre através do uso de um programa inserido através de códigos hospedados em sites maliciosos e utilizando-se de vulnerabilidades do navegador utilizado pelo usuário vítima. (CERT.BR, 2012);
- Cavalo de tróia – São programas desenvolvidos para uma função específica e aparentemente normais, entretanto que executam funções normalmente maliciosas,

, sem o conhecimento do usuário. Se utilizam do *backdoor* para acesso remoto ao micro da vítima (CERT.BR, 2012);

- Interceptação – Nesta ameaça são capturados dados de acessos legais trafegados em rede, de forma a atuar na comunicação, originalmente iniciada pela vítima;
- Interferência em consulta na base de dados – Esta ameaça é causada pela interferência em processos de consulta na base de dados, podendo causar indisponibilidade de informações;
- Modificação de dados – Nesta atividade são alteradas as informações válidas por outras, de forma ilegal;
- Negação de Serviço - Ocorre quando o atacante consegue interromper a disponibilidade de um serviço;
- *Sniffers* de rede - Utilização de ferramentas para capturar pacotes de dados trafegados na rede, ocorrendo a análise do seu conteúdo;
- Uso ilegítimo – Uso de dados válidos de forma ilegítima, geralmente após a captura das informações válidas de forma ilegal;
- Vírus - Programa ou parte de um programa malicioso, que se propaga, se tornando parte de outros programas e arquivos (CERT.BR, 2012).

Diante destas ameaças reais, os danos e indisponibilidades causados por eles em serviços de redes corporativas, podem causar os mesmos danos nas redes industriais com sistemas SCADA.

2.3.2 ANÁLISE DOS ATAQUES OCORRIDOS

Diversas ameaças cibernéticas direcionadas às infraestruturas críticas surgiram nos últimos anos, gerando ataques a diversos alvos estratégicos.

Em (JANICKE,2012) são vistos os eventos de ataques cibernéticos às infraestruturas críticas. O primeiro exemplo de ataque ocorreu na Austrália em 2000, na estação de água e esgoto de Queensland, quando ocorreu um acesso não autorizado de um funcionário ao sistema de controle.

A consequência foi um derrame de milhões de litros de esgoto em parques e rios locais.

Em 2003 a ameaça SQL *Slammer*[2] congelou os dados exibido em tempo real no painel de monitoramento da usina de Davis-Besse em Ohio – EUA, causando indisponibilidade da usina por 6 (seis) horas.

Em 2006 um ataque DoS (Negação de Serviço) causou sobrecarga de tráfego de rede na usina nuclear de Browns Ferry em Alabama – EUA, resultando em falhas nas bombas de recirculação e causando o desligamento manual da usina. O Vírus causador não foi identificado.

Em 2010 surge o Stuxnet, sendo considerado a primeira arma cibernética a explorar o sistema SCADA e o primeiro *malware* de guerra cibernética. Foi desenvolvido para atacar as infraestruturas críticas nucleares, atuando na usina de enriquecimento de urânio de Natanz - República Islâmica do Irã, na qual alterou a rotação das centrífugas, deixando sérias sequelas.

Sua principal característica é ter como alvo os sistemas de controles industriais SCADA, visando sabotar as configurações de CLP's locais (SHEARER, 2013), (BYRES e HOWARD, 2010).

Na época da sua descoberta, os motivos exatos da sua existência não foram esclarecidos, entretanto existem afirmações de pesquisadores de que a intenção mais provável seja a espionagem industrial. As prováveis características de seus criadores são as grandes qualificações técnicas e altos recursos para o desenvolvimento deste *malware*, tendo em vista sua especialidade em sistemas industriais e devido ao fato de possuir partes do seu código semelhantes aos códigos de outros *malwares*, como o Flame e Duqu (SHEARER, 2013).

O Stuxnet utiliza 5 vulnerabilidades dia-zero, ou seja, as vulnerabilidades que ainda não possuem correções dos fabricantes dos sistemas operacionais, presentes nas versões desatualizadas do sistema operacional. A partir dessas vulnerabilidades, seu objetivo é infectar o CLP (Controlador Lógico Programável) Siemens SIMATIC S7, atuando durante a execução da aplicação Siemens STEP 7, responsável por inserir a programação no CLP. Em consequência, causa a alteração na velocidade das turbinas, geradores e centrífugas de enriquecimento de urânio, conforme ocorrido no Irã (BYRES e HOWARD, 2010).

[2] SQL *Slammer* – Ataque que se baseia no ataque de negação de serviço da porta UDP1434, usada pelo sistema SQL *Server*.

Se destaca dos demais *malwares* pois seu objetivo é infectar micros específicos de operação em sistemas de controles industriais. Até o ano de 2011 infectou cerca de 50.000 a 100.000 computadores, principalmente no Irã (68%) (FALLIERE et al.,2010), conforme demonstrado na FIG. 3.1:

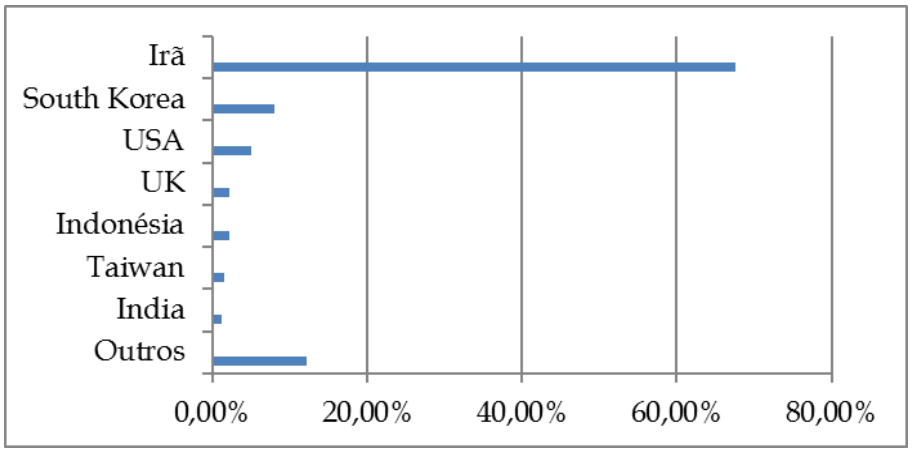

FIG. 2.2 – Percentual de Sistemas Siemens Infectados (fonte:(FALLIERE et al,2010)

As vulnerabilidades dia zero utilizadas são: MS10-046 e MS 08-067(execução de código remoto), MS10-061(spooler de impressão), MS10-073 (alteração de privilégios) e MS10-092 (Agendador de tarefas) (FALLIERE Et al., 2010).

O principal vetor de infecção do Stuxnet é a unidade de disco removível que, ao se conectar em um equipamento infectado, criam-se nela arquivos de atalhos maliciosos com extensão (*.lnk) e arquivos temporários (*.tmp), através da vulnerabilidade MS10-046. Esta vulnerabilidade permite a execução do código malicioso na criação destes atalhos, quando utilizado o Windows Explorer para visualização dos seus arquivos.

A proliferação em um equipamento ainda não infectado se inicia a partir da visualização pelo Windows Explorer destes arquivos da unidade de disco removível infectada, ocorrendo a execução de um *exploit* e em seguida dos arquivos WTR4141.tmp e WTR4132.tmp, que são arquivos *.dll codificados (MATROSOV, 2013). Arquivos*.dll possuem bibliotecas referentes aos processos vinculados a diversos sistemas, sendo de grande importância para a segurança do sistema operacional.

Ao serem executados, estes arquivos geram *drivers* maliciosos no sistema operacional que inicializam junto com o sistema, possuindo as funcionalidades de injeção de códigos nos processos válidos do sistema (MATROSOV, 2010).

A proliferação do Stuxnet em redes também ocorre pelas vulnerabilidades através de pastas compartilhadas, compartilhamento de impressão, e injeção de código remoto.

A proliferação entre computadores com pastas compartilhadas, tem a finalidade de copiar e executar o *worm* nos micros da rede, expandindo a infecção. As vulnerabilidades associadas a esta atividade são a MS 10-073 (alteração de privilégios) e MS 10-092 (Agendador de tarefas).

A proliferação entre computadores com compartilhamento de impressão é realizada através da vulnerabilidade MS10-061 (*spooler* de impressão), que permite a impressão em forma de arquivos. Devido a uma falha no *spooler* de impressão, os documentos podem ser impressos em arquivos na pasta do diretório do sistema Windows.

A proliferação usando a vulnerabilidade MS 08-067 permite a injeção de código remoto para um serviço válido do sistema operacional, gerando a cópia do principal arquivo *.dll do Stuxnet.

Esta vulnerabilidade é a mesma explorada no ataque simulado realizado neste trabalho na subseção 3.4.1.

O Stuxnet infecta a pasta de arquivos do Sistema *Step* 7 Siemens do equipamento do operador. Sua ação principal é renomear o arquivo original de *S7otbxdx.dll* para *S7otbxsx.dll* e em seguida, instalar sua própria versão maliciosa do arquivo *S7otbxdx.dll* (FALLIERE, 2010).

Este arquivo é estratégico pois é um arquivo de biblioteca usado pelo software Step 7 na comunicação e configuração do CLP. Assim, o Stuxnet consegue alterar qualquer comunicação de comandos de configuração no CLP (MATROSOV, 2010), podendo causar graves alterações nos comportamentos dos dispositivos industriais conectados ao CLP.

Em 2011 surge o Duqu, com técnicas de operação de grandes semelhanças com o Stuxnet, acreditando que tenham sido criados pelos mesmos autores (SECURELIST, 2012), (BENCSÁTH, 2012).

É desenvolvido em uma arquitetura “*Tilded*” semelhante ao Stuxnet, onde um arquivo de driver que carrega um módulo principal (biblioteca criptografada), acompanhado de arquivos de configuração maliciosos. Adicionalmente possui um

bloco codificado no registro do sistema, que injeta seus módulos em processos válidos do sistema operacional (GOSTEV, 2011).

Sua forma infecção é através de arquivos maliciosos, como um documento enviado por *email* ou inserido no equipamento por um dispositivo de disco removível. (BENCSÁTH, 2012) e (CHIEN et al., 2012). Possui semelhanças com o Stuxnet, porém seus objetivos são coletar dados dos ativos industriais, demonstrando sua característica de ciberespionagem.

Em 2012 surge o Flame, que assim como o Duqu, possui como objetivo a ciber-espionagem, como o vazamento de documentos e arquivos sigilosos (GOSTEV, 2012). Parte do seu código é idêntico ao do Stuxnet. Pesquisadores identificaram que ele já existia em 2009 e foi utilizado um módulo seu no código de desenvolvimento do Stuxnet (ZHIOUA, 2013).

Flame não possui uma forma específica de infecção inicial. Possui várias formas de ataque, como *phishing* através de *emails* ou *sites* infectados. Tem a capacidade de se autodestruir, conforme ocorreu nos seus primeiros ataques.

Os principais dispositivos infectados usados para disseminação do vírus são unidades de armazenamento removíveis e equipamentos em rede.

Possui vários módulos combinando as capacidades de um *worm, trojan e backdoor*. Tem ao menos 20 MB de tamanho, sendo este um dos motivos de ter sido ignorado pelos sistemas antivírus, por praticamente não existir vírus deste tamanho (GOSTEV, 2012).

Ao ser infectado, o equipamento se anuncia na rede local como um *proxy web.* Sendo assim, outros micros tentam acessar a *web* através dele, que recebe os pedidos de atualizações de software Microsoft e, por usar falsos certificados de segurança da empresa Microsoft, consegue enviar cópias do *malware* aos demais equipamentos (NETWORK SECURITY, 2012).

Assim, Duqu e Flame possuem grande relação com o Stuxnet, pois possuem códigos semelhantes como dele e por serem potenciais *malwares* de infraestruturas críticas, pois possuem objetivos de espionagem industrial, como vazamento de documentos, *sniffing* do tráfego de rede, coleta de dados digitados pelo do teclado e coleta dos dados de ativos industriais para possíveis futuros ataques direcionados.

Ainda em 2012 surge o Shamoon, que foi projetado para substituir e limpar os arquivos e o Master Boot Record (MBR) do computador tornando-o inutilizável.

Atacou uma organização do setor de energia no Oriente Médio, Saudi Aramco, destruindo 30.000 workstations. (ZHIOUA,2013) (RASHID, 2012);

Em 2013 pesquisadores identificaram o Havex, que foi desenvolvido pela Rússia, atuando desde 2011 em ciber-espionagem, coletando dados de informações de ativos industriais em diversos países (CROWDSTRIKE, 2013).

Na tabela 2.1 são visualizadas resumidamente as ações e consequências referentes aos ataques acima mencionados.

TAB. 2.1 – Tabela Comparativa dos Ataques

LOCAL	INFRAESTRUTURA	AGENTE	CONSEQUÊNCIA
AUS (Queensland)	Estação de Àgua	Humano	Vazamento de esgoto em rios
EUA (OHIO)	Usina Nuclear	SQL Slammer	Indisponibilidade da rede de operação por 6 horas
EUA (Alabama)	Usina Nuclear	Não identificado	DoS – Desligamento da usina
IRÃ	Usina Nuclear	Stuxnet	Aumento de 40 % na rotação da centrífuga
Hungria	-	Duqu	Roubo de dados dos ativos industriais
IRÃ	Indústria Petrolífera	Flame	Ciber espionagem
Oriente Médio	Usina Energia	Shamoon	Destruição de dados de 30.000 *workstations*
25 países EUA com maior índice	Setor Energia	Havex	Roubo de dados dos ativos industriais

Diante da análise dos ataques comparados na TAB. 2.1, pode-se constatar que os *malwares* Stuxnet, Flame, Shamoon e Havex podem ser considerados atualmente como as principais ameaças recentes às infraestruturas críticas do setor elétrico. O Duqu, mesmo não tendo atacado uma infraestrutura crítica, é considerado uma ameaça. Tal fato se justifica principalmente por existirem evidências de que tenha sido desenvolvido na mesma origem do Stuxnet e Flame, devido às semelhanças nas estruturas dos seus códigos de desenvolvimento (NETWORK SECURITY, 2012).

Por fim, o Shamoon também é uma ameaça, por ser um *malware* direcionado à destruição de dados dos ativos críticos, podendo causar graves indisponibilidades em empresas de infraestruturas críticas (RASHID, 2012), (ZHIOUA, 2013).

3 HONEYPOT PROPOSTO: HONEYSCADA

Honeypot é um simulador de serviços de rede que tem o objetivo de coletar tentativas de conexões ilegítimas. A partir da coleta das características dos ataques, pode proporcionar o desenvolvimento da segurança nos diversos sistemas. (JAIN et al., 2011).

Quanto à sua interatividade são classificados como *alta* interatividade – onde ocorre maior interação do atacante com os serviços e acesso interno ao *honeypot* e de *baixa* interatividade – no qual o ocorre somente interação com os serviços de rede do *honeypot*, não ocorrendo acesso a ele (STEDING-JESSEN, 2008), conforme TAB. 3.1.

TAB. 3.1 – Interatividade do Honeypot (Adaptado de (WADE, 2011))

Baixa interação	Alta interação
Simula serviços de rede e sistemas operacionais	Utiliza os sistemas operacionais e serviços reais
Baixo risco de danos pelo atacante aos serviços simulados	Maior risco, provendo maior interação do atacante contra os sistemas e serviços reais

Um dos mais promissores mecanismos de defesa em redes industriais, são os *honeypots,* que simulam os serviços dos CLP's (BUZA et al., 2014).

Honeypots em ambiente computacional virtualizado proporcionam restauração mais rápida em caso de indisponibilidade (TJELTA, 2011).

A arquitetura *honeySCADA* proposta neste trabalho utiliza o *honeyCLP* Conpot (RIST et al., 2011) de baixa interatividade, juntamente com um equipamento do operador, que simula interações entre eles.

3.1 DESCRIÇÃO DA ARQUITETURA

A Arquitetura *honeypot* proposta é um ambiente simulado de operação SCADA. Possui um equipamento com sistema operacional Windows XP SP3 e sistema supervisório SCADABR[3], simulando um operador de sistema SCADA interagindo com um *honeyCLP*, gerando tráfego de dados HTTP, SNMP e Modbus/TCP, conforme a FIG. 3.1:

[3] Sistema supervisório SCADABR, disponível em: http://www.scadabr.com.br

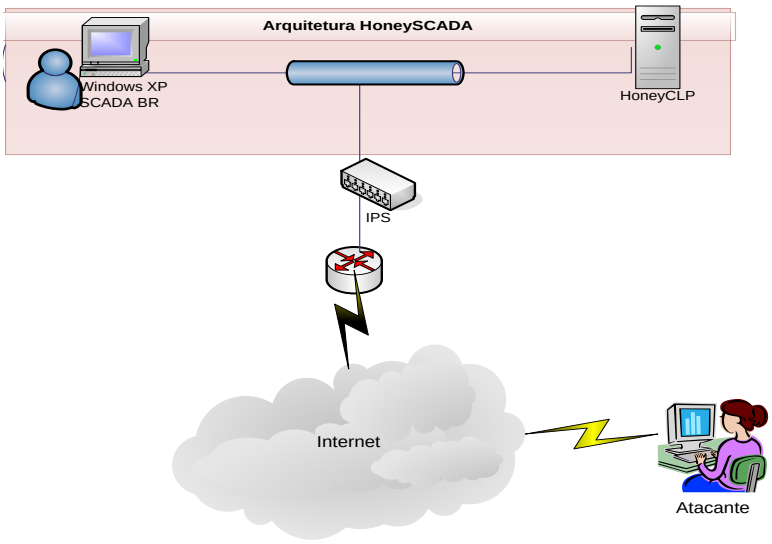

FIG. 3.1 – Arquitetura HoneySCADA

Para análise dos dados dos ataques foi utilizado um IPS, que é um Sistema de Prevenção a Intrusão com assinaturas para detecção de ataques ao sistema SCADA, na fronteira da arquitetura proposta.

3.2 CLP VIRTUAL

O projeto Conpot (RIST et al., 2011) é um *honeyCLP* lançado pelo projeto *Honeynet Project*[4] em maio de 2013, disponível para pesquisas referentes ao assunto. Este *honeyCLP* é composto por uma distribuição Linux Ubuntu 12.01, desenvolvido em linguagens de programação *Python e XML,* simulando um CLP do fabricante Siemens modelo S7, podendo ser customizado de acordo com as necessidades.

Nele são simulados 3 (três) serviços: HTTP, Modbus IP e SNMP, sendo estes dois últimos os principais protocolos usados em sistemas de controle industrial.

Foi escolhido para uso neste trabalho, por ser um lançamento recente e baseado em *software* livre.

[4] The Honeynet Project, 2011. URL: http://www.honeynet.org

Para a validação da similaridade entre o *honeyCLP* e o CLP Siemens S7 foi realizada uma avaliação dos resultados gerados pela ferramenta PLCSCAN[5] e posteriormente uma análise estatística com os dados gerados destas interações.

Esta validação se faz necessária tendo em vista que não foram identificados trabalhos de validação do respectivo *honeyCLP*, além de proporcionar resultados referentes à real atratividade do *honeyCLP* aos possíveis ataques cibernéticos.

3.2.1 VALIDAÇÃO DA SIMILARIDADE

Os fatores motivadores para a realização desta validação estatística são:

- O fato do *honeyCLP* conpot não possuir em seu projeto de pesquisa original esta validação estatística para avaliar sua similaridade com um CLP real;
- Devido a semelhança existente nos dados de saída da ferramenta PLCSCAN, após interações com os ativos *honeyCLP* e CLP Siemens.

A validação da similaridade foi realizada através de resultados obtidos com a ferramenta PLCSCAN (para identificação específica do CLP), aplicando métodos estatísticos na comparação das amostras. Estas amostras contêm dados que foram gerados a partir da interação do *honeyCLP* e o CLP Siemens com esta ferramenta, sendo coletados os *traces* pela ferramenta Wireshark[6].

A infraestrutura para realização da validação utilizada neste experimento foi estruturada simulando um ambiente no qual o atacante verifica uma rede, identificando um CLP como alvo, utilizando as ferramentas NMAP[7] (para identificação dos serviços e portas ativas dos alvos) e PLCSCAN.

As ferramentas NMAP, PLCSCAN e WIRESHARK foram instaladas em equipamento virtualizado pela ferramenta VMware, com distribuição Linux Ubuntu 12.01 para interação com o CLP Siemens S7 na mesma rede física e o *HoneyCLP* em produção exposto na INTERNET, conforme a FIG. 3.2.

[5] https://code.google.com/p/plcscan
[6] http://www.wireshark.org
[7] http://www.nmap.org

A FIG. 3.2 ilustra detalhadamente a infraestrutura utilizada, conforme citado acima:

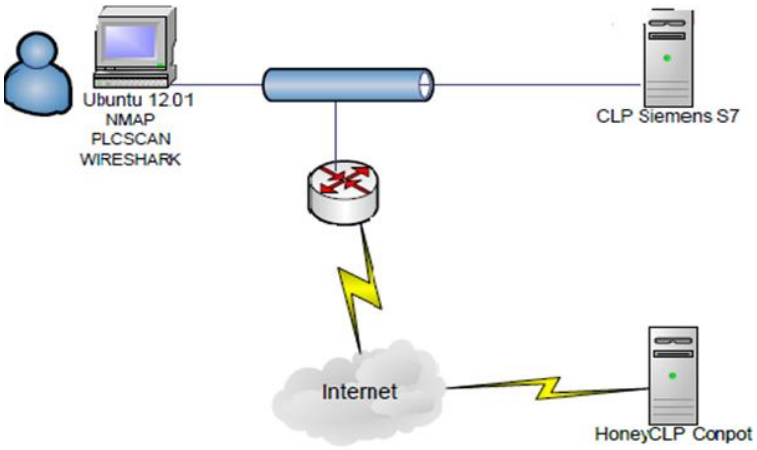

FIG. 3.2 – Arquitetura dos Experimentos de Validação

As etapas de realização do experimento foram definidas de acordo com a sequência das atividades: Execução da ferramenta NMAP, para verificação dos serviços de rede dos alvos identificados; Execução da ferramenta PLCSCAN para identificação das características do CLP e *HoneyCLP* em produção; Coleta de dados e aplicação dos métodos estatísticos.

O uso das ferramentas NMAP e PLCSCAN direcionadas aos ativos (*honeyCLP* e CLP Siemens), resultaram nos dados exibidos na TAB. 3.2 e TAB. 3.3:

TAB. 3.2 – Resultados do HoneyCLP

Ferramenta	Serviço	Porta	Dados
NMAP	HTTP	TCP – 80	TCP open HTTP
	SNMP	UDP – 161	'public' info: 'Siemens, SIMATIC S7, CPU-200, 6ES7 211-1AD30-0XB0, HW: 2, FW: V.2.2.5, SZVC6YU8207352'
	Modbus	TCP – 502	TCP open asa-appl-proto
PLCSCAN	Modbus	TCP – 502	Modbus/TCP unit ID:255
			Device info error: Slave Device Failure

Com base nestes dados, foram identificados com a ferramenta NMAP no *honeyCLP* os serviços ativos de um CLP, como o serviço Modbus IP ativo na porta

502/TCP, exibindo como resultado os dados TCP “open asa-appl-proto”, como identificação do pacote Modbus.

O serviço SNMP, que utiliza a porta UDP 161, exibe como resultado os dados de identificação do *HoneyCLP* como “Siemens, SIMATIC S7”, contendo a marca do fabricante, modelo de CPU e versões de *hardware* e *firmware*. O serviço HTTP utiliza a porta 80/TCP, exibindo os dados TCP open HTTP com resultado.

Por fim, a ferramenta PLCSCAN também identifica o serviço Modbus, atuando na porta 502/TCP, exibindo os dados Unit ID:255 como “*Slave Device Failure”.*

Isso significa que o CLP e *HoneyCLP* não possuem nenhum ativo de campo industrial (sensor, válvula etc..) conectado a ele para recebimento de comandos e configurações.

Foram realizadas alterações no *honeyCLP* visando a simulação de conexão com um ativo de uma planta industrial, sendo gerado o resultado com a ferramenta PLCSCAN, conforme abaixo:

A.B.C.D:502 Modbus/TCP
Unit ID: 255
Device: Powermeter Schneider Electric PM 9 series
Scan complete

Neste resultado é representado no texto acima o endereço IP do *honeyCLP* pelas letras A.B.C.D. Estas alterações tiveram o objetivo de tornar o ambiente *honeySCADA* mais atrativo aos ataques direcionados aos sistemas industriais, diante do resultado exibindo uma conexão do *honeyCLP* com ativos de uma planta industrial.

Os dados resultantes na TAB. 3.3 representam semelhanças entre o *HoneyCLP* e o CLP, que são identificados como dispositivos Siemens com a porta TCP/502 ativa em operação com o serviço Modbus/TCP. Diante disso, justifica-se o uso dos métodos estatísticos para analisar a similaridade das amostras coletadas.

TAB. 3.3 – Resultado do CLP Siemens S7

Ferramenta	Serviço	Porta	Dados
NMAP	Modbus	TCP – 502	TCP open asa-appl-proto MAC Address: 08:00:06:6E:E1:BB (Siemens AG)
PLCSCAN	Modbus	TCP – 502	Modbus/TCP unit ID:255 Device info error: Slave Device Failure

Com base nas amostras coletadas na saída da ferramenta PLCSCAN, são analisados todos os pacotes TCP/502 e Modbus IP existentes com a comunicação *TCP three-way-handshake* completa, direcionados ao *honeyCLP* e CLP Siemens.

Os dados excedentes das amostras coletadas identificados como pacotes TCP [RST,SYN] e TCP [spurious retransmission], são descartados da análise por representarem erros de comunicação em rede, sendo irrelevantes para obtenção dos resultados.

São definidos os parâmetros para realização da comparação entre as amostras, optando-se inicialmente pelos tamanhos da requisição e resposta, por serem considerados os que tem as características básicas de um pacote de dados. Adicionalmente foram definidos os parâmetros de intervalo entre os pacotes e TTL – *Time To Live*, para uma análise mais detalhada dos pacotes de dados a serem comparados. Assim, os parâmetros definidos para o cálculo da similaridade entre o CLP real com o *HoneyCLP* são:

1. Tamanho da Requisição;
2. Tamanho da Resposta;
3. Intervalo entre os pacotes;
4. TTL – *Time To Live* dos pacotes.

Os métodos estatísticos adotados no cálculo da similaridade das amostras de dados são o ANOVA (análise da variância) e Teste T *Student*, aplicados com a ferramenta SPSS - *Statistical Package for the Social Sciences*.

Em (HOLANDA FILHO et al., 2007) é proposto um método de identificação de anomalias, utilizando a variância como componente de importância na comparação dos dados, obtendo-se resultados satisfatórios.

Estes métodos foram escolhidos por serem utilizados amplamente nas comparações entre amostras de dados, usando-se o teste de hipóteses para avaliar a similaridade entre duas ou mais amostras. A partir da aplicação dos métodos estatísticos ANOVA e Teste T *Student* nos parâmetros de avaliação das amostras coletadas dos pacotes TCP/502 e Modbus IP, foi realizado um experimento com 10 repetições com o CLP e o *honeyCLP* , sendo gerados os resultados constantes nas TAB. 3.4 e TAB. 3.5 :

TAB. 3.4 – Experimento Estatístico Modbus IP

PARÂMETROS DEFINIDOS					RESULTADO
REQUISIÇÃO	RESPOSTA	TTL	INTERVALO	MÉTODO	SEMELHANÇA
X	X			TESTE T	100%
		X		TESTE F	100%
		X		TESTE T	100%
			X	TESTE F	100%
			X	TESTE T	100%
X	X	X	X	TESTE T	100%
X	X	X	X	ANOVA	100%
			X		100%
		X			100%
X	X				100%

As amostras da interação da ferramenta PLCSCAN foram coletadas através das 10 repetições do experimento, onde cada repetição resulta na coleta de 2 amostras (sendo uma da interação com o *honeyCLP* e outra da interação com o CLP Siemens). Os resultados das comparações dos dados Modbus IP das amostras de cada repetição demonstraram 100% de similaridade entre as amostras coletadas.

Na TAB.3.5 a comparação dos dados TCP/502 das amostras resultaram em maioria com 100% de similaridade, onde somente o teste F do parâmetro “intervalo entre os pacotes de requisição e resposta” resultou no cálculo de variância de 70% de similaridade entre as repetições do experimento.

TAB. 3.5 – Experimento Estatístico TCP/502

PARÂMETROS DEFINIDOS					RESULTADO
REQUISIÇÃO	RESPOSTA	TTL	INTERVALO	MÉTODO	SEMELHANÇA
X	X			TESTE T	100%
		X		TESTE F	100%
		X		TESTE T	100%
			X	TESTE F	70%
			X	TESTE T	100%
X	X	X	X	TESTE T	100%
X	X	X	X	ANOVA	100%
			X		100%
		X			100%
X	X				100%

A utilização do Teste F no experimento é devido à necessidade de se identificar a igualdade ou não das variâncias dos parâmetros comparados, para definição da fórmula a ser aplicada para cálculo do Teste T Student.

Por fim, nos 30% que apresentaram resultados de variâncias distintas, foram observados que os resultados do teste F nos testes possuem valores elevados se comparados com os respectivos valores nos resultados de 70% similares, além de apresentarem uma diferença entre as médias das amostras comparadas de 50% a 100%, sendo possivelmente os motivos da distinção entre as variâncias destas amostras.

3.3 OPERADOR VIRTUAL

3.3.1 ANÁLISE

O equipamento que simula um operador em atividade é caracterizado por um equipamento virtual com sistema operacional Windows XP SP3 e o sistema SCADABR simulando um operador de uma rede industrial SCADA. Na simulação do ambiente, o operador interage com um *honeyCLP*, gerando tráfegos HTTP, SNMP e Modbus IP, conforme ilustrado na figura 3.1.

Este equipamento possui a vulnerabilidade MS 08_067, que permite execução de código remotamente sobre os serviços NETBIOS e SMB, sendo uma das vulnerabilidades exploradas no ataque do Stuxnet.

Esta característica demostra grande atratividade para o recebimento de ataques cibernéticos, principalmente no caso dos ataques específicos que busquem vulnerabilidades em redes industriais.

Utilizando a ferramenta NMAP direcionada ao equipamento do operador, são identificadas outras características de um equipamento de operação de rede industrial. Na TAB. 3.6 essas características são identificadas, como o sistema operacional Windows XP SP3, juntamente com os serviços Step 7 Siemens através da porta 102/TCP ativa, resultando nos dados do protocolo "*open iso-tsap*" que são exibidos no pacote de comunicação do Step 7 (BUZA et al., 2014).

São identificadas também as portas 445/TCP e 139/TCP, utilizadas pelo SMB (*Service Message Block*) e pelo protocolo NETBIOS, que possuem utilidade de transmissão de arquivos, compartilhamento e identificação em redes Microsoft, sucessivamente.

Estes serviços estão associados à vulnerabilidade MS 08-067, existente no equipamento do operador, para atrair ataques que explorem estes serviços.

TAB. 3.6 – Dados do Micro Operador pelo NMAP

SERVIÇO	PORTA	DADOS
Siemens S7	TCP – 102	open iso-tsap
SMB	TCP – 445	open Microsoft-ds
NETBIOS	TCP – 139	open netbios-ssn
Sistema operacional	-	Windows XP SP3

Por fim, os dados da TAB. 3.6 demonstram que as características apresentadas pelo equipamento do operador são semelhantes a um equipamento de operação de sistemas industriais, sendo um alvo de grande interesse aos ataques direcionados para esse fim.

3.4 ATAQUES SOFRIDOS PELO HONEYSCADA

3.4.1 ATAQUE SIMULADO

Para a validação da arquitetura proposta, foi gerado um ataque simulado explorando a vulnerabilidade MS 08_067 do sistema operacional Windows XP, usado pelo operador na arquitetura, por ser esta vulnerabilidade um dos vetores de ataque do Stuxnet.

Foram realizados experimentos que compreendem todas as fases de execução de um ataque, sendo utilizadas as ferramentas NMAP, PLCSCAN e *Metasploit Meterpreter* (ferramenta de invasão através das vulnerabilidades) interagindo com os alvos *HoneyCLP* e equipamento do operador da arquitetura *honeySCADA.* Em (GADGE et al.,2008) são descritas as 06 (seis) fases sequenciais realizadas em um ataque: Reconhecimento; Varredura e enumeração; Acesso; Elevação de privilégio; Manter o acesso e implantação de *backdoors* para acesso remoto futuramente.

Numa perspectiva como ação inicial de um atacante, foram executadas as duas fases iniciais de um ataque que são: Reconhecimento, Varredura e Enumeração (GADGE et al., 2008) direcionadas ao *HoneyCLP.* As demais fases do ataque são realizadas a partir do acesso, especificamente no equipamento do operador, sendo identificados os serviços específicos de uma rede industrial SCADA.

De acordo com (JAIN et al., 2011) e (BUZA et al.,2014) o site *Shodanhq*[7] é uma das ferramentas *web* utilizadas por hackers na etapa de reconhecimento dos ativos industriais de sistemas SCADA, vulneráveis na internet. Conforme evidências abaixo extraídas do site, foi identificado o *honeyCLP* deste projeto como um possível alvo:

Siemens, SIMATIC S7, CPU-200, 6ES7 211-1AD30-0XB0, HW: 2, FW: V.2.2.5, SZVC6YU8207352

A partir do uso da ferramenta NMAP direcionado ao equipamento do operador, foram geradas informações sobre o mesmo, conforme os dados exibidos na TAB. 3.6. Estes dados identificam o equipamento de um operador de sistemas SCADA.

[7] http://www.shodanhq.com/host/view/ “IP”

A partir da identificação do equipamento do operador como alvo, a ferramenta *Metasploit Meterpreter é* utilizada em um equipamento com Linux, gerando o ataque direcionado ao equipamento do operador, que possui sistema operacional Windows XP SP3 com a vulnerabilidade MS08_067, citada anteriormente. Ao se concluir o acesso através da invasão por *backdoor*, foi alterado o arquivo alvo do ataque Stuxnet, que se refere a uma biblioteca do sistema operacional Windows XP.

Na seção 3.4.2 são analisadas as características e semelhanças dos ataques recebidos através da internet, direcionados especificamente aos serviços Modbus IP do *honeyCLP* e ao equipamento do operador virtual da arquitetura.

3.4.2 ATAQUES RECEBIDOS

Foram identificados através da ferramenta IPS – Sistema de Prevenção a Intrusão, diversos ataques cibernéticos e de diversas origens direcionados ao *HoneySCADA*. Os ataques recebidos foram analisados, sendo descartados alguns que não se relacionavam a possíveis ameaças direcionadas aos sistemas SCADA.

Inicialmente foram analisados os ataques direcionados ao *HoneyCLP* Conpot, com suas características analisadas conforme a TAB.3.7:

TAB. 3.7 – Ataques ao HoneyCLP Conpot

FAIXA IP PROVENIENTE DO PAÍS	ATAQUE	TOTAL
BRASIL, EUA, ALEMANHA, ARGÉLIA, INDONÉSIA	TCP SYN – PORT SCAN	14
EUA	UDP – PORT SCAN	1
BRASIL, EUA, PARAGUAY	MODBUS – Fluxo inválido de gravação	82
BRASIL	MODBUS – Leitura de requisição ao CLP	
BRASIL, RÚSSIA, ROMÊNIA, SUÍÇA, SUÉCIA	MODBUS – Leitura de Identificação do CLP	
EUA, BRASIL, CANADÁ, ESPANHA	CONFICKER	6
ARGENTINA, CHINA, ESPANHA, INDONÉSIA, ÍNDIA, SUÍÇA.	SQL SLAMMER	40
ALEMANHA, CORÉIA DO SUL, EUA, FRANÇA, HOLANDA, REP. TCHECA, SUÉCIA, UCRÂNIA	DoS	218

Os ataques acima identificados foram detectados no período de 90 dias tendo sido observadas maiores incidências de ataques de negação de serviço (DoS) e ao serviço Modbus IP. Nesse período foram identificados 82 (oitenta e dois) ataques direcionados ao serviço Modbus IP. Destes ataques, 12 (doze) foram considerados ataques críticos com o objetivo de alterar o protocolo Modbus de maneira crítica, com origens em diversos países, especificamente do Brasil, EUA e Paraguai.

Em relação aos demais 70 (setenta) ataques, 43 (quarenta e três) foram referentes a identificação do dispositivo Modbus, em que se busca detalhes como a versão do produto e fabricante do CLP, sendo caracterizada como uma ação de reconhecimento.

Os 27 (vinte e sete) ataques restantes ocorreram com o objetivo de leitura de requisições ao CLP, nos quais um cliente Modbus não autorizado tenta ler informações do CLP, HMI e dispositivos de campo que se comuniquem com ele.

Os Ataques SQL Slammer e conficker, são direcionados em sua maioria a equipamentos Microsoft Windows, sendo possíveis ameaças ao equipamento do operador do CLP em rede, não sendo considerados como ameaças aos serviços do *CLP*. Estes registros de ataques do SQL Slammer identificam que 80% são oriundos da China.

Nas etapas realizadas por um atacante existem as fases de reconhecimento do alvo e de ação efetiva. O Ataque *Port Scan* se enquadra como uma ação de reconhecimento uma vez que, através do seu resultado, pode-se definir o alvo a ser atacado, de acordo com as suas portas e serviços ativos.

Dos 15 (quinze) ataques *Port Scan* identificados, 2 (dois) deles são oriundos do mesmo IP de ataque ao Modbus IP, que foram realizados em sequência ao *Port Scan*.

Em relação aos ataques cibernéticos direcionados ao equipamento do operador da arquitetura *HoneySCADA*, foram identificados 92 (noventa e dois) ataques com maiores índices com origens entre os países da Rússia e Taiwan. Estes ataques direcionados exploram as mesmas vulnerabilidades exploradas na seção 3.4.1-Ataque Simulado, explorando as portas 445 (SMB) e 139 (NETBIOS) conforme dados da TAB. 3.8:

TAB. 3.8 – Ataques ao Equipamento do Operador

ATAQUE	QUANTIDADE	FAIXA IP PROVENIENTE DO PAÍS
SMB/NETBIOS	92	RÚSSIA, TAIWAN, UCRÂNIA, POLÔNIA, ÍNDIA E DEMAIS 20 PAÍSES.
DoS	73	EUA, HOLANDA, ROMÊNIA, POLÔNIA, ALEMANHA, REINO UNIDO
SQL Slammer	12	CHINA, TAIWAN

Foram identificados 73 (setenta e três) ataques de negação de serviço (DoS) com maior incidência dos EUA e Holanda e 12 (doze) ataques SQL *Slammer*, com origens da China e Taiwan.

Analisando os ataques que obtiveram semelhanças com o ataque simulado, foram identificados 92 (noventa e dois) ataques envolvendo os serviços SMB e NETBIOS. Entretanto, os mesmos não foram conclusivos, tendo em vista que somente foram iniciados através de um pacote de requisição de dados, porém não tiveram continuidade, conforme a TAB. 3.9:

TAB. 3.9 – Ataque SMB/NETBIOS

SIMULADO						TAM./BYTES	
N.ORD	ORIGEM	DESTINO	TIPO	TAMANHO	INFO	SMB	92
27	192.168.91.57 (Meterpreter)	192.168.91.161 (Operador)	SMB	162	Create AndX Request, **FID: 0x4008**, Path:\ Browser	NETBIOS	96
28	192.168.91.161 (Operador)	192.168.91.57 (Meterpreter)	SMB	205	Create AndX Response, **FID: 0x4008**	TCP	32
NETBIOS – SAMBA SMBD						**TAM./BYTES**	
N.ORD	**ORIGEM**	**DESTINO**	**TIPO**	**TAMANHO**	**INFO**	SMB	102
3	188.241.212.35 (Atacante)	A.B.C.D (Operador)	SMB	160	Create AndX Request, Path:\ Browser	NETBIOS	106
-	-	-	-	-	-	TCP	20

Após análise dos dados é verificado que no ataque simulado ocorre a comunicação de requisição e resposta com pacotes SMB, NETBIOS e TCP, com tamanhos de 92, 96 e 32 bytes, diferentes dos respectivos pacotes nos ataques recebidos.

A avaliação do ataque direcionado ao SMB/NETBIOS, executado por 92 vezes em períodos de tempo distintos, resulta na observação de que os pacotes de requisição dos ataques possuem tamanhos diferentes do ataque simulado, além de

diferenças entre os valores dos campos **flag2** do SMB. Entretanto, essas diferenças são comuns de acordo com o tamanho dos nomes dos arquivos gerados[8].

A Diferença observada de maior relevância é a ausência do campo **FID**[9] na comunicação de requisição dos ataques recebidos, que é necessário existir na comunicação de requisição e de resposta de forma semelhante, conforme ocorrido no ataque simulado, pois representa a identificação do arquivo a ser criado.

Esta pode ser considerada esta a causa mais relevante do ataque ter sido inconclusivo e por consequência, não ter recebido resposta aos pacotes de requisição dos respectivos ataques.

Foi realizada na TAB. 3.10 uma comparação de ataques recebidos para a validação da eficácia do equipamento do operador. Este equipamento foi comparado com um equipamento com características de sistema operacional semelhante, composto por Windows XP para o serviço de operador de sistema de tarifação de telefonia IP.

O objetivo desta comparação é demonstrar que ambos os ativos permaneceram expostos aos ataques da internet pelo mesmo período de 90 (noventa) dias, entretanto com resultados diferentes referentes aos ataques recebidos.

TAB. 3.10 – Comparação dos Ataques Direcionados

ATIVO	**ATAQUES**			
-	**SMB/NETBIOS**	**DoS**	**SQL SLAMMER**	**RDP**
Equipamento Operador HoneySCADA	92	73	12	55
Equipamento Operador Telefonia IP	-	43	10	14

Diante da análise dos dados identificados na TAB. 3.10 acima, constata-se que os ataques direcionados ao equipamento do operador foram realizados em maior quantidade.

Com exceção dos ataques SMB/NETBIOS, que ocorreram direcionados ao equipamento do operador, todos os ataques comparados na TAB.3.10 ocorreram direcionados aos 2 (dois) ativos comparados. Destes ataques, o de maior percentual

[8] http://msdn.microsoft.com/en-us/library/cc246254.aspx

[9] http://msdn.microsoft.com/en-us/library/ee442082.aspx

de diferença entre os equipamentos do operador HoneySCADA e o de Telefonia IP, foi o ataque RDP (acesso remoto), com quantidade maior que 200% entre eles.

Tal fato se deve por possivelmente ter sido identificado como um alvo de redes industriais com maior atratividade aos ataques, principalmente no que se refere a causar indisponibilidade em serviços críticos industriais.

Conforme observado, os serviços SMB/NETBIOS não foram alvo de ataques no equipamento de tarifação de telefonia IP, provavelmente pelo fato do equipamento não possuir características que o identificassem como um possível equipamento de operação de redes SCADA.

Por fim, diante dos ataques direcionados aos ativos comparados, é válida a afirmação de que o equipamento de operação de redes SCADA foi identificado como um alvo de redes industriais.

Tal afirmação se baseia principalmente por ter recebido maiores quantidades de ataques nos serviços SMB/NETIOS, explorados no ataque Stuxnet.

3.5 TRABALHOS RELACIONADOS

3.5.1 HONEYNET CLP

Em (WADE, 2011) foi implementada uma *honeynet* CLP (02 máquinas virtuais baseadas em distribuição Linux Ubuntu) composta por um *honeypot* simulando um modelo de CLP Modicon da empresa *Schneider Electric* com os serviços Modbus IP,FTP, HTTP, SNMP e Vx Debugger UDP) e por um *honeywall*, que atua na administração e captação de dados da *honeynet*.

Foram analisados os ataques ocorridos aos serviços de rede SCADA e à rede corporativa, resultando somente em ataques aos serviços de rede corporativa, não ocorrendo nenhum ataque aos serviços específicos SCADA (Vx Debugger/UDP e MODBUS IP).

Neste trabalho foi destacada a necessidade de experimentos com *honeynets* SCADA nas redes de instituições que sejam infraestruturas críticas, para fins de obtenção de melhores resultados.

3.5.2 CRYSYS CLP HONEYPOT (CRYPLH)

Em (BUZA et al., 2014) foi desenvolvido o CryPLH, que é um *honeyCLP* de alta interação, simulando um CLP Siemens S7, implementado em rede de IP público da Universidade de Tecnologia e Economia de Budapeste.

No período de um mês foram identificados diversos ataques específicos de rede corporativa direcionadas ao *honeypot*, entretanto nenhum dos ataques foram considerados expressivos e críticos de alteração ou indisponibilidade dos serviços de um CLP.

3.5.3 HONEYNET SCADA

Em (WILHOIT, 2013) foi desenvolvida uma *honeynet* SCADA de alta interação simulando um CLP Siemens S7. Em sua composição, foram distribuídos 12 (doze) *honeyCLP's* em diversos países , conforme ilustrado na TAB. 3.11.

TAB. 3.11 – Localização dos Honeypots

PAÍS	QUANTIDADE
AUSTRÁLIA	1
BRASIL	1
CHINA	2
EUA	2
IRLANDA	1
JAPÃO	1
RÚSSIA	3
SINGAPURA	1
TOTAL	**12**

Foram recebidos ataques originados de diversos países, sendo categorizados como críticos e não críticos na TAB.3.12 a seguir:

TAB. 3.12 – Ataques Críticos por Localidade

FAIXA IP	ATAQUES CRÍTICOS
ALEMANHA	1
CHINA	5
FRANÇA	1
REINO UNIDO	1
JAPÃO	1
PALESTINA	1
TOTAL	**10**

Após a implementação em diversos países, foram identificados 10 (dez) ataques críticos ao serviço MODBUS IP, dos quais tiveram maior incidência da China, que representou 50% destes ataques, seguida por Alemanha, Reino Unido, França, Palestina e Japão, todos estes com 10% dos ataques, validando os resultados da implementação dos *honeypots* desse trabalho.

3.5.4 ANÁLISE COMPARATIVA

Diante da análise dos trabalhos relacionados, desenvolvidos com objetivos semelhantes a este trabalho, contata-se através de uma comparação entre os seus resultados, que o trabalho em (WILHOIT, 2013) possui maior expressividade de forma satisfatória. Tal afirmação pode ser visualizada na TAB. 3.13, ilustrando as características entre os demais trabalhos.

TAB. 3.13 - Comparativo de ataques nas pesquisas com HoneyCLP

	M.Wade (Digitalbond)	**D.Buza (CryPLH)**	**K. Wilholt (Trend Micro)**	**Trabalho Proposto**
Modelo de CLP	Schneider Modicon	Siemens S7	Siemens S7	Siemens S7
Serviços	VxDebugger / HTTP FTP/ MODBUS IP	HTTP / FTP SNMP/S7	HTTP/FTP MODBUS IP	HTTP/SNMP MODBUS IP
Honeypot	1	1	12	1
Interação	Baixa	Alta	Alta	Baixa

Rede	Internet	Internet	Internet	Internet
Ambiente	Universidade	Universidade	Não divulgado	Setor Elétrico
Dias	38	30	90	90
Ataques Modbus	-	-	74	82
Ataques Críticos	-	-	10	12

Os trabalhos desenvolvidos em (WADE, 2011) e (BUZA et al., 2014) não obtiveram resultados referentes a ataques cibernéticos direcionados aos serviços críticos dos seus *honeypots.*

Em (WILHOIT, 2013) seus resultados apresentaram 10 ataques críticos, conforme citado anteriormente, de um total de 74 ataques ao MODBUS IP. Os 64 ataques ao serviço MODBUS IP tiveram como objetivo a identificação do dispositivo e ocorreram com maior origem da Rússia, com 43% dos ataques.

Neste trabalho foram identificados diversos ataques direcionados ao *honeyCLP* e ao equipamento do operador, sendo que este último um alvo atacado apenas neste trabalho, se comparado aos demais trabalhos relacionados.

Foram identificados 82 ataques ao serviço MODBUS IP do h*oneyCLP* Conpot utilizado, juntamente com 92 tentativas de ataques em vulnerabilidade utilizada no ataque do Stuxnet, direcionados ao equipamento do operador.

4 CONSIDERAÇÕES FINAIS

4.1 CONCLUSÃO

Este trabalho apresenta eventos de ataques direcionados às infraestruturas críticas desde o ano 2000, incluindo alguns ataques cibernéticos direcionados às infraestruturas críticas de sistemas industriais. São identificadas as ameaças e vulnerabilidades que surgiram aos sistemas SCADA, devido a interconectividade das redes industriais com as redes corporativas, fato causado pela evolução das telecomunicações integradas.

São analisadas as características de algumas ameaças às infraestruturas críticas industriais, como os ataques Stuxnet, seguido de Flame e Duqu, além das vulnerabilidades exploradas no Stuxnet.

Foi proposta uma arquitetura *HoneySCADA*, no intuito de coletar ataques para análise e comparação com os ataques analisados neste trabalho.

O *HoneyCLP* Conpot foi utilizado na arquitetura *HoneySCADA*, sendo comparado estatisticamente com um CLP Siemens S7, de forma a validar a sua similaridade com um CLP real. Foi alterado o código do *HoneyCLP* para simular o seu controle em um ativo de planta industrial, no intuito de torná-lo mais atrativo aos ataques.

O *HoneySCADA* proposto neste trabalho foi disponibilizado na rede corporativa de uma empresa da área energética, ficando suscetível aos ataques das mais diversas fontes, embora nenhum deles tenha sido expressivo. Entretanto, quando exposto ao ambiente da internet, os ataques recebidos foram específicos, visando causar danos e a indisponibilidade dos serviços.

Os ataques recebidos pelo *HoneySCADA* foram comparados com os trabalhos relacionados recentes sobre o assunto, sendo considerado satisfatório pelos seus resultados apresentados.

Por fim, nesta pesquisa é possível destacar como contribuições:

- Estudo comparativo entre trabalhos recentes voltados aos experimentos com honeypots de sistemas SCADA;
- Validação do *honeyCLP* Conpot como um sensor aplicável nos experimentos para coleta de ataques em infraestruturas críticas;

• Proposta da arquitetura *honeySCADA,* que tem como diferencial a inclusão da simulação do equipamento do operador.

4.2 TRABALHOS FUTUROS

Durante o desenvolvimento desse trabalho, foram identificados possíveis desdobramentos para trabalhos futuros:

• O desenvolvimento de *honeyCLP* simulando diversos modelos de CLP’s;

• O desenvolvimento de simuladores de outros componentes do sistema SCADA, proporcionando pesquisas que possam resultar em arquiteturas completas de redes industriais simuladas, para uso na análise de ataques cibernéticos.

5 REFERÊNCIAS BIBLIOGRÁFICAS

ABNT, 2005. ABNT NBR ISO/IEC 27002:2005: **Tecnologia da Informação: Código de Prática para a Gestão da Segurança da Informação**, 2005.

ANA. Agência Nacional de Águas. **Sistemas de Informações Hidrológicas,** 2010.

BECCUTI, M. **Quantification of dependencies between electrical and information infrastructures**. In: International Journal of Critical Infrastructures, Vol.5, p.14 – 27, Inderscience Publishers, 2012.

BENCSÁTH, B. **Duqu: Analysis, detection, and lessons learned.** In: ACM European Workshop on System Security (EuroSec), 2012.

BELLAVITA, C. **Water challenges and US national security**, May 2012.

BRANQUINHO, M.A; SEIDL, J. **Segurança de Automação Industrial e SCADA.** Editora Elsevier, 2014.

BYRES, E.; HOWARD, S. **Analysis of the Siemens WinCC/PCS7 Stuxnet Malware for Industrial Control System Professionals**. version 3.1 - October 2010. URL: www.tofinosecurity.com. Acessado em: 25/09/2012.

BUZA, D. I. **CryPLH: Protecting smart energy systems from targeted attacks with a PLC honeypot**. In: ESSOS 2014 – Engineering Secure Software and Systems, 2014.

CANONGIA, C. **International Critical Information Infrastructures Protection Handbook** 2009. Center for Security Studies, ETH Zurich, p. 36-37, 2009.

CDN/SE - Conselho de Defesa Nacional, Secretaria Executiva. **Grupo de Trabalho de Segurança das Infraestruturas Críticas da Informação**. CGSI. Brasília, 2009

CERT.BR. **Cartilha de Segurança para Internet – Códigos Maliciosos**, 2012. URL: http://cartilha.cert.br/malware/. Acessado em: 20/07/2013.

CHIEN, E.; MURCHU, L.; FALLIERE, N. **W32. Duqu: the precursor to the next stuxnet**. In: Proc. of the 5th USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET). 2012.

CHIKUNI, E.; DONDO, M. **Investigating the security of electrical power systems SCADA**. In: AFRICON 2007. IEEE, 2007. p. 1-7.

CROWD STRIKE. **Global Threat Report**. May 2013.

DE MATTOS, J.R.L.; GUIMARÃES, L. S. **Gestão da tecnologia e inovação: uma abordagem prática**. Editora Saraiva, 2005.

DHS - Department of Homeland Security – EUA. **National Infrastructure Protection Plan**, 2013.

DHS - Department of Homeland Security – EUA. **NIPP - National Infrastructure Protection Plan – Energy Sector,** 2011.

DSIC - GSI/PR. **Guia de Segurança de infraestruturas críticas da informação.** 2010.

FALLIERE, N. ; MURCHU, L. O.; CHIEN, E. **W32.Stuxnet Dossier**. Technical report, Symantic Security Response, October, 2010.

FALLIERE, N**. Exploring Stuxnet's PLC Infection Process.** Blogs: Security Response, 2010.

GADGE, J.; PATIL, A. **Port Scan Detection.** In: ICON 2008. 16th IEEE International Conference on Networks, 2008.

GHORBANI, A.; BAGHERY, E. **The state of the art in critical infrastructure protection: a framework for convergence**. In: International Journal of Critical Infrastructures, v. 4, n. 3, p. 215-244, 2008.

GOSTEV, A.; SOUMENKOV, I. **Stuxnet/Duqu: The evolution of drivers**, 2011.

GOSTEV, A. **The Flame: Questions and answers,** 2012. URL: https://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers. Acessado em: 18/10/2013.

HOLANDA FILHO, R. **Identificação da Componente de Tráfego de Ataque baseada em Discriminantes Estatísticos**. Em: V Workshop de Desempenho de Sistemas Computacionais e Comunicação SBC - Sociedade Brasileira de Computação, 2007.

HOPWOOD, D. **Flame creates heated debate**, Network Security, Elsevier, June 2012, ,URL: http://www.sciencedirect.com/science/article/pii/S1353485812700491. Acessado em: 15/01/2014.

IGURE, V.M.; LAUGHTER, S. A.; WILLIAMS, R.D. **Security issues in SCADA networks**. Computers & Security, v. 25, n. 7, p. 498-506, 2006.

JAIN, P; SARDANA, A. **A Hybrid Honeyfarm Based Technique For Defense Against Worm Attacks**, In: Word Congress of Information and Communication Technologies. Mumbai – Índia. 2011.

JANICKE, H; PATEL, T; DYER, S. **SCADA security in the light of Cyber-Warfare**, Elsevier – Computers&Security. 2012.

KANG, D. **Analysis on cyber threats to SCADA systems**. In:Transmission & Distribution Conference & Exposition: Asia and Pacific, 2009. IEEE, 2009.

LEE. J. **Challenges and Direction toward Secure Communication in the SCADA System**. Myongji University. In: 8th Annual Communication Networks and Services Research Conference - IEEE – Magazine Computer Society. 2010.

MAHBOOB, A.; ZUBAIRI, J. **Intrusion avoidance for SCADA security in industrial plants**. In: Collaborative Technologies and Systems (CTS), International Symposium on. IEEE, p. 447-452. 2010.

MANDARINO JR, R. **Segurança e Defesa do Espaço Cibernético Brasileiro**. Brasília, p. 37 - 38, 2010.

MATROSOV, A. **Stuxnet under the microscope**. ESET LLC, 2010.

MOTTA PIRES, P. S.; OLIVEIRA, Luiz Affonso. **Security aspects of SCADA and corporate network interconnection: An Overview**. In: Dependability of Computer Systems, 2006. DepCos-RELCOMEX'06. International Conference on. IEEE, p. 127-134. 2006.

MOSS, M.; TOWNSEND, A. **Telecommunications infrastructure in disasters: preparing cities for crisis communications**, New York University, New York, 2005. URL: http://www.nyu.edu/ccpr/pubs/NYUDisasterCommunications1-Final.pdf. Acessado em: 25/02/2014.

NIC - National Intelligence Council – EUA. Paper **"Global Water Security",** 2012.

PARFOMAK, P. **Vulnerability of concentrated critical infrastructure: background and policy options**, CRS Report for Congress, Congressional Research Service, Washington, DC, 2008.URL: www.fas.org/sgp/crs/homesec/RL33206.pdf. Acessado em: 06/03/2014.

RASHID, F.Y. **Disttrack Sabotage Malware Wipes Data At Unnamed Middle East Energy Organization**, 2012. http://www.securityweek.com/disttrack-sabotage-malware-wipes-data-unnamed-middle-east-energy-organization . Acessado em: 10/03/2014.

RIST, L. e VESTGAARD, J. - **Honeypot Conpot**, 2011. URL: http://www.conpot.org. Acessado em: 20/06/2012.

ROBERTS, B. **The macroeconomic impacts of the 9/11 attack: evidence from real-time forecasting**, Office of Immigration Statistics Policy Directorate, Department of Homeland Security, Washington, DC, 2009. URL: http:// www.dhs.gov/xlibrary/ assets/statistics/publications/ois_wp_impacts_911.pdf. Acessado em: 25/06/2013.

SECURELIST. **Duqu - Monthly Malware Review**, march 2012. URL: http://www.securelist.com/en/analysis/204792225/Monthly_Malware_Review_March_2012. Acessado em: 05/09/2013.

SHEARER, J. **W32. Stuxnet**. Symantec Security Response, 2013.

STEDING-JESSEN, K. **Uso de Honeypots para o Estudo de Spam e Phishing**. Tese de doutorado. INPE. 2008. URL: http://urlib.net/sid.inpe.br/mtc-m18@80/2008/08.18.19.02. Acessado em: 12/06/2013.

TJELTA, J. **Honeypots in network perimeter defense systems**.Master thesis. University of Oslo. 2011.

UNICEF – **ODM 7 – Objetivo do milênio 7 - Garantir a sustentabilidade ambiental.** 2013. URL: http://www.unicef.org/brazil/pt/resources_9612.htm. Acessado em: 25/01/2014.

VILLASENOR, J. **Securing an infrastructure too complex to understand**. The Brookings Institute Washington, 2011.

WADE, M. **SCADA Honeynets: The attractiveness of honeypots as critical infrastructure security tools for the detection and analysis of advanced threats**, Master Thesis. Iowa State University, 2011.

WHITTINGTON, J.; ARMBRUSTER, G. **Are we prepared for the economic risk resulting from telecom hotel disruptions**?, In: International Journal of Critical Infrastructures, Vol.5, p. 55 – 65, Inderscience Publishers, 2012.

WILHOIT, K. **Who's Really Attacking Your ICS Equipment?.** Trend Micro forward-Looking Threat Research Team. 2013.

ZHENDONG, M.A; SMITH, P.; SKOPIK, F. **Towards a Layered Architectural View for Security Analysis in SCADA Systems**, 2012.

ZHIOUA, S. **The Middle East under Malware Attack Dissecting Cyber Weapons**. In: Distributed Computing Systems Workshops (ICDCSW), 2013 IEEE 33rd International Conference on. IEEE, 2013. p. 11-16.