CYBERWARFARE: O SISTEMA FINANCEIRO COMO ALVO

CYBERWARFARE: THE FINANCIAL SYSTEM AS A TARGET

André Aurélio Rossi, Aluno de Segurança da Informação na FATEC Americana, andre.rossi@fatec.sp.gov.br

Marcus Vinícius Lahr Giraldi, Professor de graduação na FATEC Americana, marcus.lahr@fatec.sp.gov.br

Resumo

Este artigo tem como objetivo mostrar a evolução dos principais ataques ao sistema financeiro e como eles têm se espalhado pelo mundo. Para isso investigamos relatórios de agências de segurança, artigos e livros que tratam de casos ocorridos entre os anos 2009 e 2020, período de aumento significativo de ataques. Cada vez mais sofisticados, os ataques que, em alguns casos tentam interromper serviços ou realizar transações fraudulentas, têm como alvo, entre outros, o sistema SWIFT de mensagens. Os casos investigados, apesar da sofisticação, ainda dependem de falhas humanas para alcançar os objetivos. Assim, concluímos que é imprescindível um esforço conjunto para garantirmos a segurança da rede no território, bem como das instituições contidas nele. Isso, porque alguns ataques além do ganho financeiro também apresentam motivações políticas, o que nos coloca em um cenário de guerra cibernética.

Palavras-chave: sistema financeiro, SWIFT, guerra cibernética.

Abstract

This article has the objective to show the evolution of the main attacks on the financial system and how they have spread around the world. For this, we investigated reports from security agencies, articles and books that deal with cases that occurred between 2009 and 2020, a period of significant increase in attacks. Increasingly sophisticated, attacks that, in some cases, attempt to disrupt services or carry out fraudulent transactions, target, among others, the SWIFT messaging system. The investigated cases, despite the sophistication, still rely on human error to achieve the objectives. Thus, we conclude that a joint effort is essential to guarantee the security of the network in the territory, as well as the institutions within. This is because some attacks in addition to financial gain are also politically motivated, which puts us in a cyberwarfare scenario.

Keywords*: financial system, SWIFT, cyberwarfare.*

1. Introdução

O risco de ataques cibernéticos ao sistema financeiro cresceu a medida que o sistema se tornou mais digital e isso é evidenciado pelo aumento de incidentes. Isto traz à tona características únicas de risco pertinentes a este tipo de crime com maior potencial de afetar a estabilidade do sistema financeiro (BRANDO, 2022).

A *Financial Stability Board (FSB)* alertou, em 2020, que estes ataques podem causar instabilidades ao sistema financeiro global. A organização alerta, ainda, que nos últimos cinco anos o número de incidentes aumentou consideravelmente e que têm tido grande impacto nas instituições financeiras e também no ecossistema onde operam. Incidentes que, caso não sejam contidos adequadamente, podem interromper serviços, atingir infraestruturas criticas para o funcionamento do sistema financeiro, diminuir a confiança do público, minar a integridade de todo o sistema, além de causar prejuízos para investidores e para o público em geral (MAUER, 2020).

Embora atualmente seja comum ler sobre ataques ao sistema financeiro coordenados por países, estes ataques são relativamente novos. Entender a evolução destes ataques ajuda a compreender como estes ataques atingiram o estágio atual de detalhamento e sofisticação. Ataques desta natureza demonstram ser uma grande ameaça pois, diferente de grupos independentes, estes grupos possuem recursos financeiros e tecnológicos que os possibilitam desabilitar ou evitar sistemas robustos de segurança (BAE SYSTEMS, 2017).

Estes ataques têm como alvo, *sites*, serviços voltados ao público, caixas eletrônicos e o sistema financeiro de mensagens: *Society for Worldwide Interbank Financial Telecommunications* (SWIFT). Atualmente, ataques a instituições financeiras são mais sofisticados, avançados e executados com mais sutileza (SWIFT, 2021).

Considerando os ataques cibernéticos ao sistema financeiro, o presente artigo tem como objetivo perscrutar casos significativos de invasão, entre os anos 2009 e 2020, nos quais os grupos mostraram persistência, inovação, criatividade e conhecimento para atingir seus objetivos.

2. Referencial Teórico

Passamos a identificar agora os tipos de invasões, configuradas como ataques ao sistema financeiro, e suas consequências imediatas.

2.1. Ataques ao Sistema Financeiro

Atualmente, a avaliação de que ataques cibernéticos representam uma ameaça a estabilidade do sistema financeiro é axiomática, não é uma questão de se, mas quando (MAUER, 2021).

2.1.1. Ataques DDoS

Em 2009, *sites* de bancos nos EUA e na Coreia do Sul pararam de responder, em um ataque DDoS que utilizou cerca de 50.000 computadores controlados por *hackers*. O objetivo não era roubar dinheiro, mas deixar os serviços dos bancos inoperantes. Isso fez com que os usuários não pudessem usar cartões, sacar dinheiro nos caixas eletrônicos ou usar a agência bancária. O ataque usou um *malware,* que posteriormente seria nomeado Dozer, devido aos nomes encontrados nos arquivos (MILLS, 2009).

> O ataque em si foi inteligente principalmente porque se propagou usando um *worm* que se espalhou para outros sistemas automaticamente. (...) Mesmo um simples *worm* pode compartilhar um *malware* e outros componentes maliciosos rapidamente, levando à infecção máxima sem muito trabalho. Além disso, os invasores não precisaram interagir com nenhuma parte dos sistemas manualmente. (DIMAGGIO, 2022).

Os invasores conduziram três ondas de ataque DDoS entre 4 e 9 de julho, cada uma em um conjunto diferente de *sites*, incluindo domínios relacionados a finança: *banking.nonghyup.com, ezbank.sinham.com, ebank.keb.co.kr, www.nyse.com, www.nasdaq.com, finance.yahoo.com, www.usbank.com e www.ustreas.com* (DIMAGGIO, 2022). Ainda de acordo com o autor, diferente de um ataque originado por um grupo independente, o *malware* possuía características únicas: embora o ataque tenha iniciado no dia 4 de julho, ele estava programado para terminar no dia 10 de julho, cessando o ataque DDoS e iniciando o segundo componente do ataque. A tarefa deste componente era apagar arquivos com extensões específicas do sistema e depois apagar também o *master boot record (MBR)* deixando os sistemas inutilizáveis. Quando finalizada esta tarefa, o *malware* apresentava a mensagem “Em memória do dia da independência”. A mensagem anti Estados Unidos se mostra uma pista de que o ataque não partiu de um grupo independente. No

momento dos ataques, a especulação pública colocou como principal culpado a Coreia do Norte. Em 2014, o governo dos Estados Unidos confirmou essa suspeita.

DiMaggio (2022) conclui que este ataque contribuiu para mudar a percepção dos invasores para uma nova forma de causar problemas ao sistema financeiro. Um problema como esse persistindo por um longo período de tempo poderia afetar a confiança dos usuários no sistema financeiro. Em última análise, se os cidadãos desconfiados do sistema financeiro fizessem mais saques do que depósitos, um efeito em cascata poderia afetar a economia local, porém, em uma grande e consolidada economia, esse objetivo seria muito difícil de ser atingido.

Dois anos depois, outro ataque similar aconteceu tendo também como alvo instituições financeiras na Coreia do Sul. Esse ataque, assim como em 2009, também se deu em 3 etapas: primeiro, os computadores foram infectados; segundo o ataque DDoS e terceiro, destruição dos arquivos. Seguindo os mesmos passos, esse ataque derrubou servidores de bancos, e os *sites* pararam de responder.

De acordo com *Washington Post*, cerca de 30 milhões de usuários ficaram impedidos de usar caixas eletrônicos ou qualquer serviço *online* por vários dias (WASHINGTON POST, 2011).

Apesar das semelhanças, na segunda etapa havia uma diferença: a maneira como se configurou o ataque DDoS. Em 2009, o *malware dozer* se comunicava com um servidor controlado pelos invasores de onde obtinha as instruções e parâmetros de configuração, por exemplo a lista de alvos. Essa comunicação deveria passar pela rede da vítima até chegar ao servidor controlado pelos invasores. Se essa comunicação, por qualquer motivo, fosse interrompida o componente responsável pelo ataque DDoS não saberia como agir. Entretanto, nesta nova versão, o componente responsável pelo ataque DDoS já estava configurado com a lista de alvos dispensando assim a comunicação externa. Em um relatório sobre o caso, publicado pela McAfee, chama a atenção dos analistas que a sofisticação do ataque combinado a uma execução relativamente limitada e um resultado obtuso, levaram a crer que se tratava de um exercício para testar e observar a capacidade de resposta do adversário (MCAFEE, 2011).

Além disso, também estava programado para ter uma data para início e fim, neste caso seriam 10 dias. O ataque ficou conhecido como *Ten days of rain* (Dez dias de chuva).

Nestes dois casos, é possível observar que, ainda que estejam utilizando a mesma forma de ataque, há uma adaptação na execução das etapas com intuito de diminuir as chances de mitigar o ataque. Isso implica que os dois anos que separam os ataques foram usados para entender melhor como o adversário se comporta e como ele reage a partir da ocorrência. Nos dois casos, não houve tentativa de ganhos financeiros e isso associado ao tempo que separam os ataques sugerem que os responsáveis possuem outras formas de financiamento e que suas motivações são politicas.

O procurador sul-coreano responsável pela investigação creditou estes ataques à Coreia do Norte afirmando ser este um ato de ciberterrorismo sem precedentes. A Coreia do Norte, através de sua agencia nacional de notícias, nega qualquer envolvimento no ataque (WASHINGTON POST, 2011).

Ainda em 2011, outro ataque DDoS a instituições financeiras merece atenção, pois diferente dos outros, este ataque iniciou-se no final de 2011, continuou em 2012 e 2013, afetando cerca de 50 instituições financeiras nos Estados Unidos. Embora ataques DDoS não necessitem de muita habilidade para serem executados, ninguém, até então, havia tido sucesso em um ataque tão abrangente e longo como este. Relatórios sobre o incidente denotam que os bancos foram atingidos com 140Gbps de dados, fazendo deste o ataque DDoS mais intenso registrado até então. Dentre as instituições afetadas, estão grandes grupos financeiros como JPMorgan Chase, Wells Fargo e o *Bank of America* (TRIBUNAL DISTRITAL DOS ESTADOS UNIDOS DISTRITO SUL DE NOVA IORQUE, 2016).

Assim como em outros casos, não houve motivação financeira, apesar das vítimas serem instituições financeiras, e a continuidade dos ataques por um longo período de tempo levou as autoridades a acreditaram que este era o caso de um grupo associado a algum país. De fato, um grupo iraniano intitulado *Izz ad-Din al-Qassan Cyber Fighters* assumiu a responsabilidade pelos ataques, mas fontes do serviço de inteligência dos Estados Unidos atribuíram os ataques ao governo iraniano. Ainda de acordo com as autoridades, este caso representa uma forma de retaliação do governo do Iran, já que este sofria sanções do governo estadunidense devido ao seu programa nuclear e ao incidente com as centrifugas responsáveis pela extração do urânio para o programa nuclear do Iran. O governo do Iran responsabiliza tanto os Estados Unidos quanto Israel pelo incidente com as centrífugas do programa nuclear do Iran (NEW YORK TIMES, 2013).

Novamente, agora em 2013, a Coreia do Sul seria alvo de um ataque. Desta vez, os quatro maiores bancos do país e três grandes emissoras de notícias tiveram seus serviços interrompidos.

Mais uma vez, usuários dos bancos ficaram impossibilitados de usar caixas eletrônicos, e os funcionários não puderam usar os terminais dos bancos para ajudar os clientes, fazendo com que estes não tivessem acesso a sua conta bancária. Os *sites* dos bancos funcionaram de forma intermitente ou demoravam para responder, e as emissoras relataram que toda a rede estava fora do ar. Como em outros ataques, o *malware* usado também possuía um componente responsável por apagar arquivos específicos do sistema infectado, mas, desta vez, ele foi usado de uma maneira diferente. Após infectar diretamente os alvos desejados, como os servidores de *sites* e de instituições financeiras, os arquivos foram apagados tornando serviços críticos indisponíveis, fazendo com que o ataque tivesse o mesmo efeito de um ataque DDoS. Para infectar os alvos desejados, os invasores usaram e-mails *spear-phishing* e *sites* comprometidos. Além destes vetores, foi usada uma terceira e mais criativa, também mais efetiva, forma de infecção: uma atualização. Isto permitiu que o número de sistemas infectados, cerca de 48.700, fosse o suficiente para atingir os efeitos desejados (DIMAGGIO, 2022).

O jornal *The Register,* que cobriu o caso, diz que os *hackers* conseguiram credencias da empresa Ahnlabs que fornecia soluções de segurança e também um *software* para gerenciamento de atualizações de correção. Em posse dessas credencias, os invasores puderam distribuir o *malware* como atualização de correção passando por *firewalls* e antivírus sem ser detectado (THE REGISTER, 2013).

Mas não é só isso que torna esse ataque diferente dos demais, dois detalhes técnicos o tornam único. Primeiro, os invasores projetaram um *malware* capaz de infectar vários sistemas operacionais. Normalmente, ambientes corporativos usam sistemas Microsoft no lado do usuário, e sistemas baseados em Unix são usados em servidores, bancos de dados. Isso fez com que o componente do *malware,* responsável por apagar os arquivos, fosse capaz de atingir tanto sistemas Windows como sistemas baseados em Unix, como AIX, HP Unix, Linux e Solaris, que, muitas vezes, são usados para autorizar e coordenar a troca de informações em transações bancárias. A segunda característica que diferencia este *malware* é que ele era capaz de procurar e desabilitar programas específicos de antivírus. Se a vítima

tivesse instalado em seu sistema antivírus das empresas Hauri ou AnhLabs, o *malware* só seria executado após desabilitar os antivírus para garantir que não seria detectado. Esse ataque ficou conhecido *DarkSeoul* (MARTIN, 2015).

Esse *malware* é digno de nota, pois usou vários vetores para atingir um grande número de sistemas, era capaz de atingir diversos tipos de sistemas operacionais e evitar antivírus. Isso significa que quem estava por traz deste ataque dedicou tempo, esforços e recursos antes de executar esta operação.

Ainda de acordo com o jornal de *The Register*, apesar da falta de provas concretas, a sofisticação associada a todas as características únicas do *malware*, além das semelhanças entre outros casos conhecidos e de uma série de pistas deixadas pelo *malware,* que apontavam para grupos independentes que, até o momento do ataque, não existiam e reivindicaram o ato, são marcas que denotam um ato executado por um país. A teoria predominante é que esta foi uma resposta vinda da Coreia do Norte advindas de semanas anteriores de tensão com a Coreia do Sul (THE REGISTER, 2013).

Outro caso de ataque ao sistema financeiro, agora em 2014, um grupo *hacker* pró-Rússia autodenominado *Cyber Berkut* roubou e publicou informações sobre os clientes de um dos maiores bancos comerciais da Ucrânia, o *PrivatBank.* Entre as informações publicadas, estavam número de telefones, informações das contas e informações confidencias de passaportes. O grupo ainda informou aos clientes que estes deveriam transferir o dinheiro para outros bancos, caso contrário, corriam o risco de perder o acesso ao dinheiro (THE MOSCOW TIMES, 2014).

De acordo com o *National Cyber Security Centre,* uma organização do governo do Reino Unido que aconselha e dá suporte ao setor público e privado em como evitar ameaças de segurança, *Cyber Berkut* é um grupo, que junto com outros grupos, estão associados com o Serviço Militar de Inteligência Russa (NATIONAL CYBER SECURITY CENTRE, 2018).

> O banco nunca se recuperou completamente do ataque ou da perda de clientes, que provavelmente perderam a confiança na capacidade do banco em proteger seu dinheiro. Em dois anos, o disastre forçou o governo da Ucrânia a assumir as operações do banco para evitar falência, forçando a nacionalização do banco (DIMAGGIO, 2022).

2.2. Ataques ao Sistema SWIFT

Pelo menos oito ataques de alto nível aconteceram nos últimos anos tendo como alvo o sistema SWIFT. Todos resultaram em perdas significativas ao sistema financeiro. Somados estes ataques resultaram em uma perda de aproximadamente $167.210.000 milhões de dólares, sendo o ataque ao banco de Bangladesh um dos mais elaborados e a maior soma já roubada até então (F-SECURE, 2020).

2.2.1. Roubo Bilionário

No ano de 2016, um grupo *hacker* planejou um ataque que por pouco não obteve sucesso. A vítima era o Banco Central de Bangladesh, e o valor do roubo, $1 bilhão de dólares. Foi apenas por um acaso que o grupo não conseguiu roubar todo o planejado, mas, mesmo assim, conseguiram sair com $81 milhões de dólares (BBC, 2021).

De acordo com a *British Broadcasting Corporation* (BBC), os indícios apontavam para Coreia do Norte e um grupo apoiado pelo governo chamado *Lazarus Group*. Pouco se sabia sobre o grupo, mas o *Federal Bureau of Investigation* (FBI) conseguiu detalhar um dos suspeitos: Park Jin-hyok também conhecido como Pak Jin-hek e Park Kwang-jin.

Então em 8 de junho de 2018, o departamento de justiça dos Estados Unidos apresentou uma queixa-crime contra Park Jin-hyok. Na queixa, estavam detalhes de como o ataque se desenvolveu e os passos seguidos pelo grupo: reconhecimento, comprometimento inicial da rede, observação e aprendizado, classificação e privilégios da rede, preparação do ambiente (criação de contas e recursos), execução de transações fraudulentas e eliminar evidências.

2.2.2. Reconhecimento

O departamento de justiça dos Estados Unidos (2018) relata que Park realizou um trabalho de reconhecimento há pelo menos um ano antes do ataque ao banco de Bangladesh. Durante o reconhecimento, os invasores adquiriram informações da infraestrutura de acesso público do banco e endereços de e-mail associados. Pesquisaram o *site* do banco e funcionários, incluindo contas de rede social. Em algumas situações, usaram um serviço especializado em localizar contas de e-mail associadas a um domínio e companhias especificas.

Os invasores coletaram e-mails a fim de criar uma lista para ser usada na etapa seguinte do ataque. Em alguns casos, criaram contas falsas para imitar alguém conhecido pelo alvo. Em outros, criaram e-mails para usar em contas de redes sociais e interagir com funcionários do banco criando e-mails *spear-phishing*. Além disso, mapearam a infraestrutura pública do banco procurando por vulnerabilidades que pudessem explorar e ter acesso nas etapas seguintes (DEPARTAMENTO DE JUSTIÇA USA, 2018).

2.2.3. Comprometimento da Rede

Vários roubos atribuídos à Coreia do Norte usaram engenharia social na forma de e-mails *spear-phishing* para comprometer e ganhar acesso a rede alvo. Os atacantes criaram estes e-mails para atingir indivíduos e contas especificas identificadas durante o reconhecimento (BBC, 2021).

De acordo com as investigações do departamento de justiça dos Estados Unidos (2018), em vários ataques de alto nível, os *hackers* norte-coreanos criaram e-mails que refletiam associações conhecidas ou interesses das vítimas e usavam formatos, imagens e nomenclaturas corretas para imitar e-mails legítimos que a vítima pudesse receber. Isso evidencia que os invasores gastaram tempo e recurso para criar e-mails específicos que possuíssem relevância e aparentariam ser legítimos para a vítima.

Empresas com frequência possuem endereços de e-mail voltados para o público que não são direcionados a um indivíduo específico dentro da instituição, mas são gerenciados por um grupo ou por um administrador responsável. Durante o reconhecimento, os invasores identificaram um e-mail que era usado para enviar currículos e então enviaram um currículo com um *malware*. No corpo do e-mail, havia *link* que levava ao currículo e, após acessar o *link*, o *malware* comprometeria o sistema deixando aos invasores acesso ao sistema e à rede. Uma vez tendo acesso à rede, os invasores usavam um *malware* específico *(keylogger)* para coletar credenciais das contas de e-mail. Com estas informações, os invasores usavam estas contas para criar e-mails *spear-phishing* e enviavam para outros funcionários do banco usando contas legítimas. Para aumentar a legitimidade do e-mail, muitas vezes os invasores adicionavam outros e-mails no encaminhamento e "com cópia", demostrando o nível de detalhamento e planejamento (DEPARTAMENTO DE JUSTIÇA USA, 2018).

2.2.4. Observação e Aprendizado

Baseado no comportamento observado em outros ataques, *hackers* norte-coreanos são pacientes e passam uma quantidade de tempo considerável dentro da rede do alvo antes da execução. Em alguns casos, os invasores passam meses observando e aprendendo sobre os sistemas, e como eles se conectam com outros recursos bancários. O objetivo é entender as políticas e procedimentos do banco para saber como os funcionários lidam e conduzem transações financeiras. O aprendizado com a observação foi importante, pois permitiu aos invasores identificar maneiras de disfarçar transações fraudulentas com as atividades legítimas do banco. Esse tempo desprendido com aprendizado foi essencial para execução do roubo. Alguns bancos trabalham de forma diferente no que diz respeito ao armazenamento das transações bancárias. O banco de *Tien Phong Bank* (Vietnam) e o banco de Bangladesh armazenavam transações feitas através do sistema *SWIFT* de forma diferente. O banco de Bangladesh imprimia cópias das transações realizadas. Estas cópias forneciam evidências físicas que eram armazenadas no banco. O banco de *Tien Phong* armazenava estas cópias em arquivos digitais em um servidor terceirizado fora da instituição (DIMAGGIO, 2022).

2.2.5. Classificação e Privilégios da Rede

O objetivo desta etapa era classificar os sistemas que eram usados para enviar e receber as transações do sistema SWIFT e obter privilégios nestes sistemas. Como parte das práticas de segurança, a instituição implementava uma política de segmentação de tarefas, a fim de prevenir que uma única pessoa tivesse acesso completo aos sistemas críticos da instituição. Isto não preveniu os invasores de obterem acesso a estes sistemas críticos, mas dificultou o ataque. Essa segmentação usada pela instituição impôs aos invasores a necessidade de acessarem várias contas protegidas antes de obter acesso aos sistemas associados com as transações SWIFT (DEPARTAMENTO DE JUSTIÇA USA, 2018).

2.2.6. Preparação do Ambiente

Para preparar o ambiente para execução, os invasores precisavam que suas atividades passassem despercebidas. O tráfego de informações gerado pelo *malware,* que se comunicava tanto com a infraestrutura da vítima quanto com servidores controlados pelos invasores, poderia chamar atenção dos administradores da rede. Assim os invasores tiveram que esconder sua atividade e criaram um protocolo customizado que se confundisse com

tráfego TLS.

TLS é uma abreviação para *Transport Layer Security*, um protocolo criptografado usado para proteger a comunicação da rede, mas a versão customizada usada pelos invasores possuía um cabeçalho alterado com um conjunto de algoritmo criptográfico *(cipher suit)* que tornava a comunicação difícil de ser detectada. Além desta versão do protocolo, os invasores criaram uma outra que era responsável pela comunicação do *malware* com os servidores controlados pelos invasores. A comunicação feita com os servidores controlados pelos invasores usava uma *backdoor,* também customizada, que adicionava mais um nível complexidade, uma vez que o *malware* responsável pela *backdoor* executava na memória do sistema dispensando a necessidade de escrever no disco e deixar rastros da sua execução. O problema com esse tipo de abordagem é que, se o sistema for desligado ou reiniciado, o *malware* deixa de existir. Contudo, para contornar esse problema, o *malware* foi programado para monitorar o sistema e identificar essas ações. Caso fosse identificado algum desses dois eventos, o *malware* criaria uma cópia no disco da vítima e reinstalaria novamente após o sistema ser restaurado, depois disso, ele apagaria a cópia do disco e voltaria a existir apenas na memória do sistema (DEPARTAMENTO DE JUSTIÇA USA, 2018).

O *malware* possuía ainda outras funções que o permitiam agir como *proxy* enviando comandos para outros sistemas comprometidos, aceitando e enviando comandos de *upload* e *download* de arquivos, listar e apagar arquivos e listar, iniciar e terminar processos.

2.2.7. Execução das Transações Fraudulentas

Até este momento os invasores haviam obtido acesso a rede, observado os sistemas, aplicativos usados e processos do banco e também criaram contas para poder usar os sistemas do banco como usuários legítimos. Neste ponto há uma falha na segurança do banco que ajudou os invasores a progredirem no ataque. Normalmente o sistema SWIFT opera em uma rede separada dos demais sistemas do banco, contudo, no banco de Bangladesh não havia essa segmentação de rede e também não estavam presentes dispositivos de segurança como roteadores ou firewall. Caso estes dispositivos de segurança estivessem presentes, os responsáveis pela rede poderiam ter notado a criação de usuários com permissões de acesso ao sistema SWIFT (DIMAGGIO, 2022).

Com tudo pronto os invasores puderam então iniciar as transações fraudulentas.

Como as transações foram feitas usando usuários com autorização e acesso ao sistema SWIFT ninguém suspeitou de sua legitimidade. Usando este método os invasores tentaram executar 35 transações fraudulentas.

2.2.8. Eliminar Evidências

Métodos e procedimentos associados as transações SWIFT variam para cada banco. Da perspectiva do invasor, se um funcionário ou qualquer sistema do banco identificar as transações, isso poderia comprometer a fraude. Para contornar esse problema, os invasores acrescentaram ao *malware* um recurso capaz de apagar arquivos e outras evidências, que pudessem deixar rastros incluindo, tentativas de *login* ao aplicativo SWIFT *Alliance* e a bancos de dados associados.

Em outros ataques atribuídos à Coreia do Norte, é comum encontrar recursos implementados nos *malware* para apagar arquivos embora não iguais, mas variantes com a mesma finalidade. De fato, as características encontradas em vários aspectos do *malware* usado no banco de Bangladesh são parecidas com outros ataques, por exemplo o ataque que a Sony Pictures Interteinment sofreu em 2014.

Como relata o jornal inglês *The Guardian,* em dezembro de 2014, um grupo norte-coreano divulgou informações sobre a *Sony Pictures Entertainment* e exigiu que a empresa cancelasse o lançamento de um programa de comédia que encenava o assassinato do líder norte- coreano, Kim Jong-un. Em declaração, o FBI diz que após uma analise técnica do *malware* é possível associá-lo a outros *malware* que o FBI tem conhecimento, que foram desenvolvidos pelos norte-coreanos. Entre as características comuns, estão similaridades entre linhas específicas do código, encriptação dos algoritmos, métodos para apagar arquivos e comprometer redes (THE GUARDIAN, 2014).

Dentre todas as semelhanças encontradas no *malware* estava a função de apagar com segurança, uma característica comum encontrada em todos os ataques a instituições financeiras que tinha a tarefa de apagar seus rastros quando sua função estivesse concluída (DIMAGGIO, 2022).

2.2.9. Resposta do Banco de Bangladesh

Quando o banco de Bangladesh descobriu o roubo eles iniciaram a investigação do

que havia acontecido. Naquele momento, o governador do banco ainda acreditava que podia recuperar o dinheiro e, por isso, manteve o evento em segredo do público e do próprio Governo. Enquanto investigavam o ocorrido, descobriram que os invasores tiveram acesso ao sistema SWIFT do banco, mas o sistema SWIFT não havia sido comprometido, pois os invasores criaram contas para usarem o sistema, assim para o sistema todas as transações eram legítimas (BBC, 2021).

Neste caso, há um fator complicador, a rede do banco não tinha todos os requisitos necessários de segurança. Para os sistemas SWIFT, é recomendado que ele esteja em uma rede separada, segmentada, além de um *firewall* para proteção externa. O banco de Bangladesh não atendia a nenhum destes requisitos (CONGRESSIONAL RESEARCH SERVICE, 2017).

A situação só não se agravou ainda mais, porque do outro lado da transação estava o FED *Federal Reserve System* (FED). Conforme foi relatado, uma palavra mal escrita chamou a atenção de um funcionário do banco que imediatamente entrou em contato com banco de Bangladesh que cancelou a transação. Além disso, um sistema autônomo presente no FED interrompeu a maior parte das transferências, pois os invasores haviam criado quatro contas bancárias para onde o dinheiro seria transferido, e a agência bancária, em que as contas foram criadas, ficava em uma rua chamada Júpiter. Júpiter, porém, era o nome de uma embarcação iraniana que sofrera sanção do governo estadunidense. Quando o sistema identificou a palavra Júpiter, ele interrompeu todas as transações relacionadas chamando a atenção dos funcionários do FED (BBC, 2021).

Infelizmente para o banco, embora a maior parte das transações tivessem sido interrompidas, apenas $16 milhões foram recuperados. Dos $951 milhões que os invasores tentaram transferir com ações fraudulentas, conseguiram levar $81 milhões de dólares.

2.3. Casos Relacionados

De acordo com DiMaggio (2022), devido às semelhanças, foi possível relacionar o grupo responsável pelo ataque ao banco de Bangladesh a outros ataques ao sistema financeiro.

2.3.1. Sonali Bank

O caso aconteceu em 2013 e, de acordo com o relato, os invasores usaram um *malware* para coletar credenciais dos usuários. Após obterem acesso ao sistema SWIFT, realizaram transferências fraudulentas no valor de $250.000 dólares (F-SECURE, 2020).

2.3.2. Banco del Austro

Novamente usando um *malware* para coletar credencias, os invasores obtiveram credenciais de um funcionário e, com ela, puderam acessar sua conta de e-mail. Com a conta de e-mail do funcionário, os invasores localizaram pedidos de transações do sistema SWIFT rejeitadas e canceladas, alteraram os detalhes e as reenviaram resultando em pedidos legítimos de transferência no valor de $12.000.000 milhões de dólares (F-SECURE, 2020).

2.3.3. Tien Phong Bank

Neste ataque, os invasores usaram um *malware* especificamente criado para um leitor de arquivos PDF, Foxit, que era usado pelos funcionários do banco para ler declarações do sistema SWIFT. Os invasores conseguiram instalar uma versão modificada do leitor de arquivos na estação de trabalho de um dos funcionários que sempre que abria uma declaração, o leitor alterava a declaração com objetivo de esconder qualquer atividade ilegal. Apesar de ser considerado um ataque sofisticado e bem planejado, os funcionários do banco identificaram mensagens suspeitas do sistema SWIFT e entraram em contato com as partes envolvidas, impedindo os pedidos de transferência no valor de $1.130.000 milhões de dólares serem completados (F-SECURE, 2020).

Além destes casos, ainda existem outros que também se relacionam, seja pela semelhança em sua execução ou por similaridades no *malware*. Dentre estes casos, estão o *Far eastern international bank, Central bank and Banorte, City union bank, Banco de Chile, Globex state bank* na Rússia.

3. Metodologia

Presente artigo procurou desenvolver uma discussão sobre como ocorrem as invasões no sistema financeiro ao redor do mundo, entre os anos de 2009 e 2020.

Recorremos a um levantamento bibliográfico desses eventos e também a consulta de documentação de instituições específicas que atuam na segurança do cyber espaço. As

invasões escolhidas estão inseridas em um contexto cujas características apresentam especificidades de planejamento em sua execução. Assim, tais características despertaram nosso interesse seja pela sofisticação do planejamento ou por terem sido bem-sucedidas.

Dessa forma, a pesquisa se desenvolveu em um processo de seleção de informações disponibilizadas por instituições e agências de segurança na internet bastante limitadas, já que se trata de um tema ainda pouco relatado e discutido. Por isso, a seleção da bibliografia física sofreu também com a escassez de obras sobre o assunto. Explicar e detalhar esse tipo de assunto pode aguçar o interesse de outros grupos em realizar ataques cibernéticos ou mesmo aperfeiçoá-los. Daí o cuidado de agências e instituições na divulgação dessas informações.

O período selecionado para pesquisa foi escolhido em função do aumento nos casos de invasão ao sistema financeiro, mais suscetíveis aos ataques em função da vulnerabilidade encontrada e da divulgação das informações.

Outrossim, a guerra cibernética configura-se como uma disputa entre grupos financiados por países e, portanto, um ato de guerra. Se comprovada, é possível que tenhamos desdobramentos políticos, tais como embargos, sanções e etc. Por isso, o cuidado com qual o tema é tratado, por instituições e agências, até ser comprovado um ataque.

4. Resultados e Discussões

Os bancos cada vez mais estão se tornando digitais, e a pandemia acelerou ainda mais esta transformação. É inegável que o uso de computadores e sistemas inteligentes facilitam e agilizam as atividades tanto para clientes como para o próprio sistema financeiro. Mas isso, também aumenta os riscos uma vez que aqueles que podem causar problemas já não estão mais só nas redondezas, mas sim espalhados pelo mundo.

Considerando um cenário onde a guerra cibernética *(cyberwarfare)* é um fato, e algumas nações estão empenhando grandes esforços nessa nova forma de guerra, a preocupação com a segurança das instituições financeiras públicas ou privadas é essencial. Ainda que neste artigo tenha abordado apenas ataques ao sistema financeiro, a ameaça está presente em qualquer sistema conectado a rede de computadores. Os casos envolvem espionagem, roubo e sabotagem em Ministérios, Embaixadas, Exército, planos de saúde, organização de trabalhadores, emissoras,

enfim, qualquer lugar onde se possa obter informações sobre uma determinada população, ganhos financeiros ou prejudicar negócios.

Uma consequência ainda mais preocupante dos investimentos de nações em guerra cibernética é que, uma vez que os casos se tornam públicos e seus métodos são estudados, grupos independentes aprendem e usam estes métodos, o que aumenta o espectro de pessoas com conhecimento a táticas sofisticadas de invasão e recursos para burlar os sistemas de segurança. Assim, em um cenário onde os inimigos eram nações em conflito, agora passam a ser qualquer instituição em qualquer lugar do mundo.

Um reflexo do atual crescimento do segmento digital, ou seja, o uso cada vez maior da rede de computadores acentuado pela pandemia, é que, em 2021, o custo com incidentes de segurança aumentou em 12% e atingiu seu maior valor em 17 anos (IBM, 2022). O setor que mais sofreu aumento foi da saúde, seguido pelo setor financeiro. Mas isso não significa que o setor financeiro deixou de ser visado por invasores. O que aconteceu é que outros setores com menos investimento em segurança passaram a ser alvos “fáceis” para sequestro de dados e demanda de pagamento e com uma pandemia e governos financiando cuidados médicos, nada mais lucrativo de que este seguimento.

O setor financeiro, contudo, é palco de ataques sofisticados e criativos e o caso do banco de Bangladesh demonstram a importância de sistemas de segurança e de profissionais capacitados para lidar com esse cenário. Segundo a BBC, o ataque ao banco de Bangladesh é algo digno de Hollywood, não fosse um roubo, claro. Os invasores se prepararam antes da execução, estudaram os funcionários, coletaram credenciais, criaram contas legítimas, aprenderam sobre a política do banco, observaram como as transações eram feitas, criaram *malware* customizados, disfarçaram a comunicação entre protocolos seguros de rede e então, quando tudo estava preparado, o grupo esperou por quase um ano quando uma combinação de fim de semana e feriado que lhes dariam quase cinco dias sem que as duas instituições envolvidas pudessem ter contato. Não fosse um sistema autônomo e uma palavra mal escrita, o grupo teria sucesso no roubo.

Nos casos de ataques de alto nível relatados, o alvo sempre é o sistema SWIFT, contudo, a rede SWIFT não é comprometida, o acesso ao sistema acontece através de contas legítimas criadas a partir de credenciais adquiridas em uma rede comprometida. Isso acontece normalmente por falha humana que permite que um *malware* se instale na rede e colete credenciais de funcionários tirando proveito de uma segurança de rede mal estruturada.

Diante deste e de outros casos de ataque que visavam os sistemas SWIFT, a cooperativa lançou o programa *Customer Security Programme (CSP)* para ajudar e orientar os bancos em como se proteger destas tentativas de invasão. O programa introduzido em 2016 tem como objetivo prover suporte para instituições no combate a ameaças cibernéticas. Como parte do programa, instituições financeiras são obrigadas a avaliar sua conformidade com uma lista de controles de segurança consultivas e obrigatórias, e atestar conformidade dos controles obrigatórios anualmente.

Para guiar as instituições financeiras nestes controles foi criado o *Customer Security Controls Framework*, e em 2021estabelecia três objetivos, subdivididos em oito princípios:

Quadro 1 – Objetivos e princípios do Customer Security Controls Framework

Objetivo	Princípios
1. Proteja o ambiente de rede	P1. Restrinja o acesso a Internet
	P2. Segregar sistema críticos dos demais sistemas
	P3. Reduzir vulnerabilidades e exposição a ataques
	P4. Assegurar fisicamente o ambiente de rede
2. Saiba e Limite o acesso	P5. Previna o comprometimento de credencias
	P6. Gerencie identidades e segregue privilégios
3. Detecção e Resposta	P7. Detecte atividades anômalas no sistema ou registro de transações
	P8. Planeje resposta ao incidente e o compartilhamento de informações

Fonte: https://www.swift.com/myswift/customer-security-programme-csp/security-controls

As instituições também são incentivadas a verificar as informações de conformidades atestadas por outras instituições para conhecimento de quais instituições estão em conformidade com o programa. O objetivo é ajudar obter mais informações sobre quais instituições tem controles mais efetivos criando um mapa de quais instituições estão mais suscetíveis a ataques.

Mas ainda que seguidas as orientações, como foi demonstrado ao longo do artigo, os métodos e ferramentas usadas nas invasões estão sempre evoluindo se tornando mais sofisticadas e criativas, fazendo com que as práticas de segurança também estejam em constante evolução.

5. Considerações Finais

Atualmente, os ataques usam combinações de *malware* especificamente criados para obter credenciais e burlar requisitos de autenticação, aprender como acontecem as operações bancárias, para criar disfarces e enganar a segurança da rede apagando arquivos de *log* e qualquer rastro dos ataques. Isto deixa claro que estes invasores têm investido recursos e tempo considerável, planejando e se preparando para os ataques, em alguns casos como o banco de Bangladesh, permaneceram sem ser detectados por quase um ano dentro da rede antes de executarem as transações fraudulentas.

A determinação e a sofisticação demonstradas nos ataques ao sistema financeiro evidenciam a importância do profissional de cyber segurança. De acordo com *Cybersecurity Workforce Study (ISC)* de 2022, existe uma defasagem de 3,4 milhões de profissionais em todo mundo e mais de 300 mil no Brasil (ISC, 2022).

Segundo um relatório anual encomendado pela IBM, nos últimos cinco anos o custo de violação de dados aumentou em 12%, passando de 3,92 milhões em media. Com um aumento cada vez maior do impacto financeiro das violações de dados, isso significa também um custo cada vez maior para o público, assim o dinheiro que poderia circular na economia, sendo convertido em consumo ou investimentos, está sendo usado para conter o crime.

Sem dúvida a guerra cibernética é atualmente uma das ameaças mais graves, considerando a rede de computadores. Grupos isolados, sem auxilio de uma organização mais abrangente capaz de coletar informações de vários setores e reuni-las para que possam ser utilizadas por organizações ou público em geral, tornam-se mais suscetíveis a invasões. Isoladamente estes grupos mesmo com alto investimento em segurança não seriam capaz de conter as ameaças, tendo em vista o alto investimento de países em guerra cibernética e constante evolução nos métodos usados nos ataques.

Considerando o que foi demonstrado e discutido, é aconselhável um esforço entre Governo e instituições públicas e privadas, a exemplo da *National Cyber Security Centre* na Inglaterra. Fundada em 2016 com sede em Londres essa organização é uma colaboração entre outros grupos como a *National Authority for Information Assurance (CESG), Centre for Cyber Assessment, CERT UK* e o *Centre for Protection of Natural Infraestructure.* A organização é responsável por entender e detalhar problemas de segurança cibernética criando guias que se tornam disponíveis para organizações e para o público em geral do Reino Unido. É também responsável por responder

a incidentes de segurança cibernética e ajudar organizações para reduzir os danos causados, reduzir os riscos de rede no Reino Unido colaborando na segurança de rede em setores públicos e privados, além de usar informações da indústria e acadêmicas para aumentar a capacidade de segurança no país. Assim, diminuir as ameaças a todos os sistemas conectados em rede, inclusive ao sistema financeiro.

Ao adotarmos uma iniciativa desta natureza, tornaríamos o impacto financeiro sobre as instituições menor e contribuiríamos para aumentar a confiança do público em serviços *online*.

Referências

BAE SYSTEMS. The evolving cyber threat to the banking community. Reino Unido, 2017. Disponível em: https://www.baesystems.com/en/cybersecurity/feature/the-evolving-cyber-threat-to-the-banking-community. p. 1-3. Citado na página 2.

BBC. The Lazarus heist: how North Korea almost pulled off a billion-dollar hack. Reino Unido: Londres, 2021. Disponível em: https://www.bbc.com/news/stories-57520169. Citado nas páginas 8, 9, 12 e 13.

BRANDO, D; KOTIDIS, A.; KOVNER, A.; LEE, M.; SCHREFT, S. L. Implications of cyber risk for financial stability. New York, 2022. Disponível em: https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html. Citado na página 1.

CHANLETT-AVERY, E.; ROSEN, L.; ROLLINS, J.; THEOHARY, C. North Korean cyber capabilities**:** In brief. Washington DC: Congressional Research Service, 2017. Disponível em: https://sgp.fas.org/crs/row/R44912.pdf. p. 6. Citado na página 12.

DEPARTAMENTO DE JUSTIÇA USA. United States of America v. PARK JIN HYOK**.** Estados Unidos: Califórnia, 2018. Disponível em: https://www.justice.gov/opa/press-release/file/1092091/download. 179 p. Citado na página 8, 9, 10 e 11.

DIMAGGIO, Jon. The Art of Cyberwarfare: An Investigator's Guide to Espionage, Ransomware, and Organized Cybercrime. São Francisco: No Starch Press, 2022. p. 35-52. Citado na página 3, 4, 6, 7, 9, 11, 12 e 13.

F-SECURE. Threat analysis**.** Helsinki: Finlândia, 2020. Disponível em: https://www.f-secure.com/content/dam/f-secure/en/business/common/collaterals/f-secure-threat-analysis-swift.pdf. Citado nas páginas 13 e 14.

HARLAN, C.; NAKASHIMA, E. Suspected North Korean cyber attack on a bank raises fears for S. Korea, allies. Washington DC: Washington Post, 2011. Disponível em: https://www.washingtonpost.com/world/national-security/suspected-north-korean-cyber-attack-on-a-bank-raises-fears-for-s-korea-allies/2011/08/07/gIQAvWwIoJ_story.html. Citado nas páginas 4 e 5.

IBM, 2022. https://www.ibm.com/reports/data-breach. Citado na página 15.

ISC, 2022. https://www.isc2.org/-/media/2A313135414E400FA0DBD364FD74961F.ashx. p. 3. Citado na página 17.

LAUGHLAND, O.; RUSHE, D. Sony cyber attack linked to North Korean government hackers, FBI says. Reino Unido: The guardian, 2014. Disponível em: https://www.theguardian.com/us-news/2014/dec/19/north-korea-responsible-sony-hack-us-official. Citado na página 11.

LEYDEN, J. South Korea data-wipe malware spread by patching system. Inglaterra: Londres, 2013. Disponível em: https://www.theregister.com/2013/03/25/sk_data_wiping_malware_latest/. Citado nas páginas 6 e 7.

MARTIN, D. M. Tracing the lineage of darkseoul. Estados Unidos, 2015. Disponível em: https://www.giac.org/paper/gsec/31524/tracing-lineage-darkseoul/126346. p. 2-9. Citado na página 6.

MAUER, T.; NELSON, A. International strategy to better protect the financial system against cyber threats. Massachusetts, 2020. Disponível em: https://carnegieendowment.org/2020/11/18/international-strategy-to-better-protect-financial-system-against-cyber-threats-pub-83105. p. 11. Citado na página 1.

MAUER, T.; NELSON, A. The global cyber threat. IMF, 2021. Disponível em: https://www.imf.org/external/pubs/ft/fandd/2021/03/pdf/global-cyber-threat-to-financial-systems-maurer.pdf. p. 25. Citado na página 2.

MCAFEE. Ten days of rain: expert analysis of distributed denial-of-service attacks targeting South Korea. Califórnia: Santa Clara, 2011. Disponível em: https://www.mcafee.com/wp-content/uploads/2011/07/McAfee-Labs-10-Days-of-Rain-July-2011.pdf. p. 3-7. Citado na página 4.

MILLS, E. Botnet worm in DOS attacks could wipe data out on infected PCs. Califórnia: São Francisco, 2009. Disponível em: https://www.cnet.com/news/privacy/botnet-worm-in-dos-attacks-could-wipe-data-out-on-infected-pcs/. Citado na página 2.

NATIONAL CYBER SECURITY CENTRE. Reckless campaign of cyber attacks by Russian military intelligence service exposed. Inglaterra: Londres, 2018. Disponível em: https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed. Citado na página 7.

PERLROTH, N.; HARDY, Q. Bank hacking was the work of iranians, officials say. New York: New York Times, 2013. Disponível em: https://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html. Citado na página 5.

SWIFT. Customer security programme. Bélgica: La Hulpe, 2021. Disponível em: https://www.swift.com/myswift/customer-security-programme-csp. Citado na página 1.

THE MOSCOW TIMES. Cyber Berkut hackers target major Ukranian bank. Rússia: Moscou, 2014. Disponível em: https://www.themoscowtimes.com/2014/07/04/cyber-berkut-

hackers-target-major-ukrainian-bank-a37033. Citado na página 7.

TRIBUNAL DISTRITAL DOS ESTADOS UNIDOS DISTRITO SUL DE NOVA IORQUE. United States of America v. Ahmad Fathi, Hamid Firoozi, Amin Shokohi, Sadegh Ahmadzadegan, omid Ghaffarinia, Sina Keissar and Nader Saedi. Estados Unidos: Nova Iorque, 2016. Disponível em: https://www.justice.gov/opa/file/834996/download. p. 4. Citado na página 5.