INSIGHTS DE CIBERSEGURANÇA PARA SETORES NO BRASIL

heimdall
security research

SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

1 Por que a cibersegurança deve ser assunto fudamental para o setor financeiro.

O setor financeiro, responsável por transações bilionárias diariamente, se tornou um dos alvos mais atrativos para cibercriminosos. A crescente digitalização, impulsionada pelo uso de tecnologias como blockchain, inteligência artificial e sistemas de pagamento móvel, ampliou significativamente a superfície de ataque.

Prova disso, os últimos anos registraram um aumento expressivo na atividade de grupos de ransomware, APTs e cibercriminosos organizados. Empresas como bancos e seguradoras, foram alvo de mais de 20 mil ataques cibernéticos, que causaram um prejuízo de US$ 12 bilhões, de acordo com relatório do Fundo Monetário Internacional (FMI).

Mas por que o setor é o alvo preferido dos cibercriminosos?

A motivação por trás desses ataques pode variar desde extorsão financeira, danos que pode gerar um efeito cascata que afeta outras áreas da economia e até espionagem industrial, tornando a compreensão das ameaças ainda mais complexa. Além das perdas financeiras diretas, as consequências podem incluir danos à reputação, perda de confiança do cliente e sanções regulatórias.

Os cibercriminosos vem explorando uma ampla variedade de táticas, técnicas e procedimentos (TTPs) para comprometer os sistemas financeiros.

Ataques incluem phishing direcionado, ransomware, Advanced Persistent Threats (APTs), invasões de redes por meio de explorações em sistemas críticos, roubo de identidade e interrupção das operações, refletindo assim a importância de investir na proteção de dados.

Acompanhe neste e-book, elaborado pela equipe de Inteligência de Ameaças da ISH Tecnologia, Heimdall, uma visão abrangente das ameaças que essasinstituições enfrentam.

Veja os principais indicadores de comprometimento e como você pode antecipar possíveis incidentes, reforçando suas estratégias de defesa cibernética com reforço de políticas de acesso e atualização de sistemas.

2 Principais tipos de ameaças e motivações

Diferentemente de outros setores, como o de água e saneamento, que podem ser afetados por falhas em atualizações e manutenção, os ataques ao setor financeiro são caracterizados por sua alta complexidade e precisão.

Isso se deve ao seu papel estratégico na economia global e ao potencial impacto de uma invasão bem-sucedida, o que torna esse setor extremamente atrativo para cibercriminosos.

O volume de ataques reportados contra instituições financeiras supera significativamente o de outros setores, principalmente devido ao elevado retorno financeiro e estratégico para os atacantes.

Além disso, o setor é alvo não apenas de cibercriminosos comuns, mas também de grupos patrocinados por Estados-nação, que buscam informações e vantagens econômicas.

Diante desse cenário, é possível categorizar os principais atores de ameaça em diferentes grupos:

CIBERCRIMINOSOS:

Esses atores realizam, com frequência, ataques de ransomware e fraudes financeiras, visando obter lucro imediato. Seu foco está em explorar vulnerabilidades em sistemas bancários, gateways de pagamento e plataformas de transações, com o objetivo de extorquir grandes somas de dinheiro ou comprometer informações sensíveis, como dados de clientes e detalhes de transações financeiras.

Eles agem de forma rápida e oportunista, adaptando suas táticas para aproveitar brechas na segurança do setor.

GRUPOS DE ESTADO-NAÇÃO:

Com operações cibernéticas altamente sofisticadas, as motivações vão além do ganho financeiro direto, incluindo objetivos políticos e econômicos.

Eles direcionam seus ataques a bancos centrais, bolsas de valores e grandes instituições financeiras, buscando desestabilizar economias ou roubar informações estratégicas para ganhos de longo prazo. Um exemplo notável é o grupo Lazarus, que possui um histórico significativo de ataques contra o setor financeiro global.

Acompanhe a seguir uma análise detalhada dos principais atores de ameaças no setor, com foco em suas táticas e técnicas, baseada nas pesquisas mais recentes.

3 Conheça os grupos de cibercriminosos

Com o objetivo de fornecer insights sobre as ameaças emergentes, acompanhe uma análise de casos reais de ataques cibernéticos que impactaram o setor de recursos hídricos e saneamento.

3.1 Ransomwares

3.1.1 Ransomware Black Basta

O grupo de ransomware Black Basta se consolidou rapidamente como um dos principais atores de ameaças no cenário atual. Desde sua aparição em meados de 2022, ganhou notoriedade pela sofisticação e eficácia de seus ataques.

Operando em um modelo de Ransomware-as-a-Service (RaaS), ele permite que cibercriminosos afiliados utilizem sua infraestrutura para executar ataques. Esses afiliados têm acesso ao ransomware e a outras ferramentas necessárias para comprometer redes e extorquir vítimas, compartilhando uma porcentagem dos resgates com os administradores do grupo.

Sua abordagem segue um padrão conhecido como: após comprometer a rede da vítima, o grupo exfiltra os dados e implanta o ransomware. Caso o resgate não seja pago, os dados roubados são publicados em sites de vazamento controlados pelo grupo, adotando a estratégia de extorsão dupla.

O grupo é conhecido no financeiro por criptografar empresas do setor e exigir pagamentos para liberar a chave necessária para recuperar os arquivos criptografados.

O diferencial do Black Basta está em sua rápida adaptação a novas táticas de ataque e em sua infraestrutura técnica robusta, tornando suas operações difíceis de mitigar e rastrear. Com a crescente sofisticação de seus métodos, o grupo permanece uma ameaça significativa no cenário global de cibersegurança.

Figura 1 – Cadeia de ataque simplificada do Black Basta.

A seguir mencionamos algumas das principais vulnerabilidades identificadas como exploradas pelo grupo ou seus afiliados.

ID CVE	DESCRIÇÃO
CVE-2024-1709	Vulnerabilidade de desvio de autenticação no ConnectWise ScreenConnect.
CVE-2020-1472	Vulnerabilidade de elevação de privilégio no Netlogon (também conhecida como Zerologon).
CVE-2021-42278	Vulnerabilidade de elevação de privilégios do Active Directory Domain Services.
CVE-2021-42287	Vulnerabilidade de elevação de privilégios do Active Directory Domain Services.
CVE-2021-34527	Vulnerabilidade de execução remota de código (RCE) no Windows Print Spooler (PrintNightmare).
CVE-2024-37085	Vulnerabilidade de bypass de autenticação no VMware ESXi.

Tabela 1 – Vulnerabilidades exploradas pelo Ransomware Black Basta.

3.1.2 Ransomware Qilin

O Qilin Ransomware, também conhecido como Agenda, é uma ameaça cibernética que opera no modelo de Ransomware-as-a-Service (RaaS).

Lançado em julho de 2022, o Qilin se destaca pela alta capacidade de personalização e pelo uso estratégico de técnicas de dupla extorsão.

Além de criptografar os dados da vítima, os operadores exfiltram informações sensíveis, ameaçando publicá-las caso o resgate não seja pago, aumentando a pressão sobre as organizações alvo.

Uma característica marcante do Qilin é sua adaptabilidade a diferentes sistemas operacionais, sendo capaz de atacar ambientes Windows, Linux e até mesmo sistemas ESXi. O ransomware é escrito em linguagens como Golang e Rust, tornando suas variantes mais complexas e difíceis de detectar e analisar.

O Qilin permite que seus afiliados personalizem os ataques, possibilitando, por exemplo, a escolha de quais processos encerrar ou quais diretórios ignorar durante a criptografia, aumentando a precisão e a eficácia da ofensiva.

Em termos de método de ataque, o Qilin frequentemente obtém acesso inicial por meio de e-mails de phishing e credenciais comprometidas. Uma vez dentro do sistema, ele se movimenta lateralmente pela rede utilizando ferramentas como PsExec, e realiza a exfiltração de dados antes de iniciar a criptografia. Essa abordagem garante que os operadores possuam informações críticas para aumentar as chances de sucesso na extorsão.

Além disso, o Qilin mantém uma presença ativa na dark web, onde recruta afiliados e anuncia seus serviços. O grupo é conhecido por cumprir suas ameaças, publicando os dados roubados em sites de vazamento caso o resgate não seja pago, intensificando a pressão sobre as vítimas. Essa combinação de táticas avançadas, adaptabilidade técnica e estratégias de pressão faz do Qilin uma ameaça séria no cenário atual de cibersegurança.

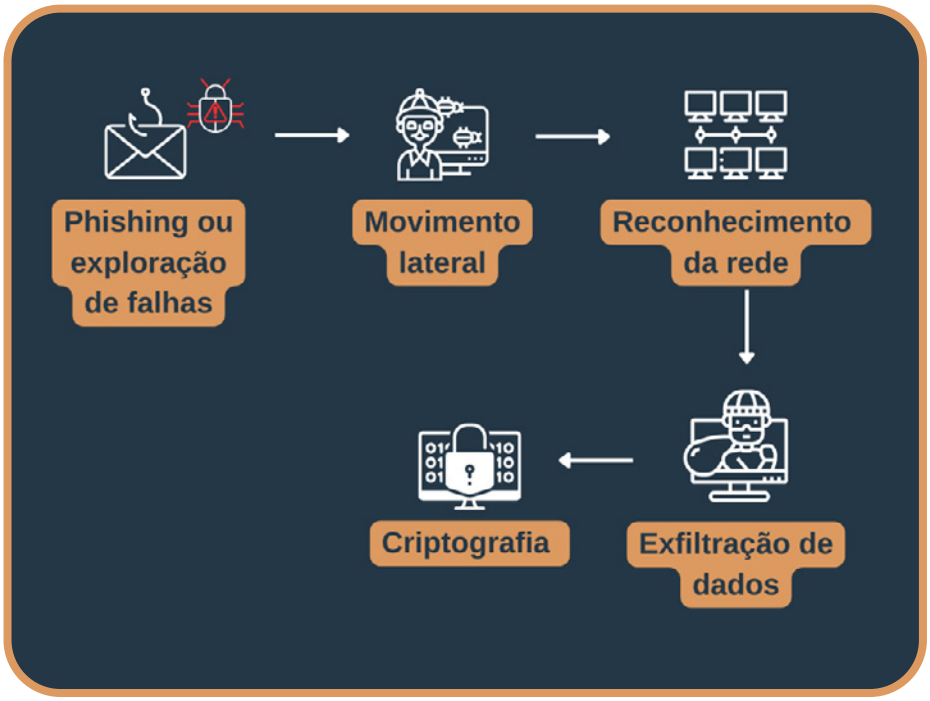

Figura 2 – Fluxo de ataque utilizando-se de phishing ou falha pelo Ransomware Qilin.

Vale destacar que o grupo, conforme mencionado anteriormente, é reconhecido por explorar vulnerabilidades de forma eficaz. Durante a análise, foi possível identificar um padrão em seu método de exploração, bem como as principais vulnerabilidades que costumam ser alvo de seus ataques.

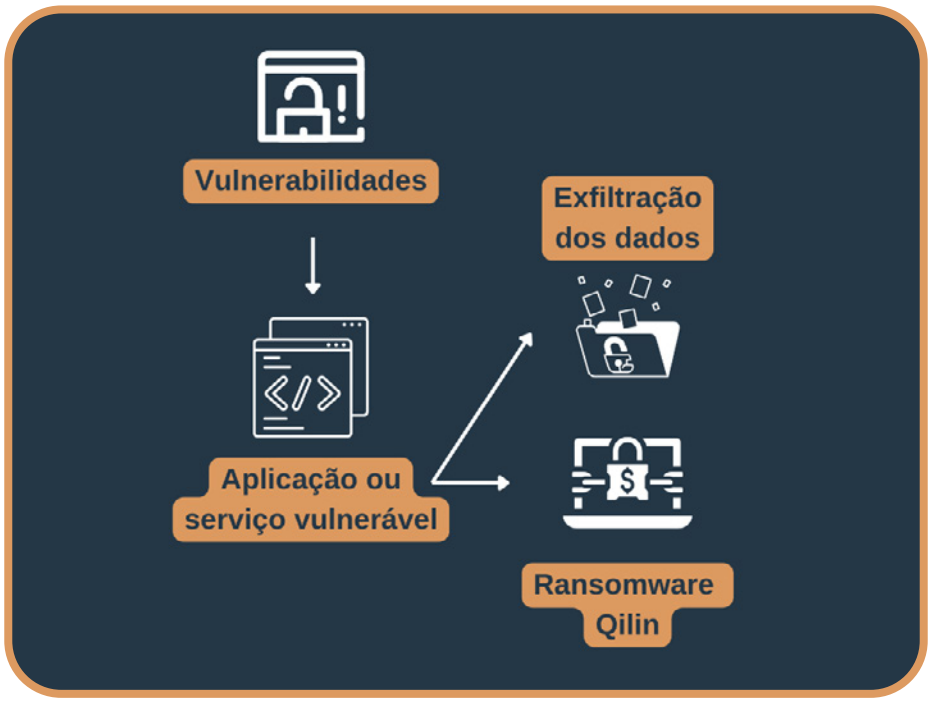

Figura 3– Fluxo de exploração de vulnerabilidade resultando em criptografia do Qilin.

ID CVE	DESCRIÇÃO
CVE-2023-27532	Vulnerabilidade no componente Veeam Backup & Replication.
CVE-2024-37085	Vulnerabilidade de bypass de autenticação no VMware ESXi.
CVE-2023-28252	Vulnerabilidade de elevação de privilégio do driver do sistema de arquivos de log comum do Windows.

Tabela 2 – Vulnerabilidades explorada pelo Ransomware Qilin.

3.2 TROJANS BANCÁRIOS

3.2.1 Malwares Bancários (Grandoreiro e PixPirate)

Um dos malwares mais notáveis já criados é o **Grandoreiro,** um dos trojans bancários mais ativos na atualidade. O malware teria surgido em meados de 2017, inicialmente visando o Brasil e o Peru, e se expandiu posteriormente para o México e a Espanha em 2019.

Como qualquer outro trojan bancário desenvolvido para atacar instituições brasileiras, o Grandoreiro possui funcionalidades de backdoor, com a capacidade de:

- ☑ **Manipular janelas (Windows);**
- ☑ **Autoatualizar-se;**
- ☑ **Capturar teclas (keylogging);**
- ☑ **Simular ações do mouse e teclado;**
- ☑ **Redirecionar a vítima para URLs maliciosas;**
- ☑ **Desconectar ou reiniciar a máquina da vítima;**
- ☑ **Bloquear o acesso a sites específicos.**

Essa versão foi projetada especialmente para sistemas operacionais Windows. No entanto, a evolução do cibercrime financeiro levou ao desenvolvimento de malwares para outras plataformas, como o **PixPirate,** voltado para dispositivos Android.

PixPirate é um trojan de acesso remoto (RAT) com foco financeiro, que utiliza diversas técnicas para monitorar as atividades da vítima e roubar informações sensíveis, como credenciais bancárias, dados de cartões de crédito e logins de diversas contas. Diferentemente do Grandoreiro, o PixPirate opera em dispositivos Android através de arquivos APK (Android Package) e pode realizar ações como:

- ☑ **Manipular e controlar outros aplicativos;**
- ☑ **Registro de teclas (keylogging);**
- ☑ **Acessar contas registradas no telefone;**
- ☑ **Acessar a lista de contatos e chamadas em andamento;**
- ☑ **Identificar a localização do dispositivo;**
- ☑ **Implementar técnicas anti-análise (anti-virtual machine e anti-debugger);**
- ☑ **Garantir persistência após a reinicialização do dispositivo;**
- ☑ **Divulgar o malware via WhatsApp;**
- ☑ **Ler, editar e excluir mensagens SMS;**
- ☑ **Se proteger contra remoção e desativação do Google Play Protect.**

3.2.2 Mekotio

Mekotio é um malware especializado em roubo de credenciais, conhecido por suas operações altamente sofisticadas e persistentes. Detectado pela primeira vez em 2023, ele utiliza técnicas avançadas de phishing e spear-phishing para infectar suas vítimas, visando principalmente organizações financeiras e grandes corporações. Sua atividade tem sido especialmente prolífica no Brasil, Chile, México, Espanha e Peru.

O que diferencia o Mekotio é sua notável habilidade em evitar a detecção. Ele emprega métodos como o uso de certificados digitais falsificados e execução diretamente na memória, evitando deixar rastros no disco.

As operações do Mekotio têm causado enormes prejuízos, principalmente no setor financeiro, onde o roubo de credenciais pode resultar em perdas financeiras substanciais. Sua capacidade de adaptação e evolução constante o posiciona como uma das ameaças mais perigosas no cenário atual da cibersegurança.

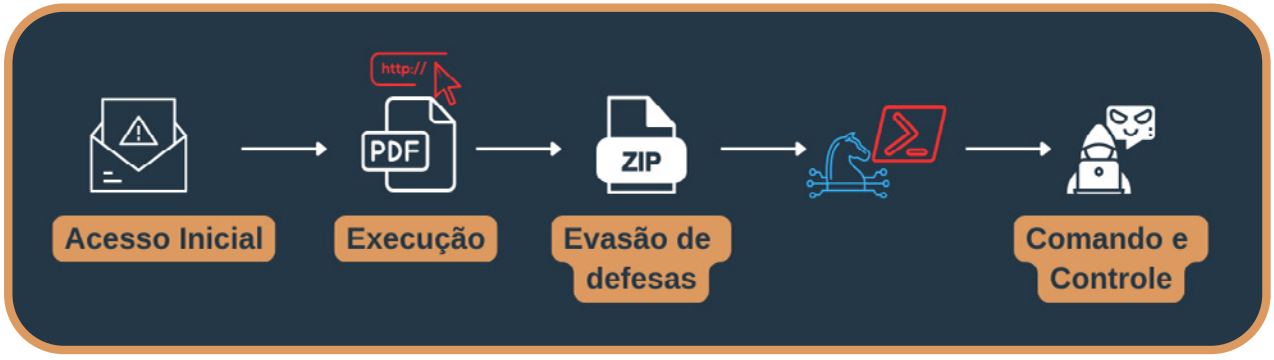

Figura 4 – Cadeia de ataque da utilização do malware.

3.3 Outros grupos que chamam a atenção

3.3.1 Grupo FIN7

O grupo FIN7, também conhecido como Carbanak Group, é uma organização cibercriminosa altamente sofisticada, ativa desde pelo menos 2015. Inicialmente, ganhou notoriedade por ataques em grande escala ao setor financeiro, usando campanhas de spear-phishing para roubar dados de cartões de crédito e informações bancárias.
Seu modus operandi envolve o uso de malwares personalizados, como Carbanak e Cobalt Strike, para infiltrar redes corporativas e exfiltrar dados sensiveis.

Nos últimos anos, o FIN7 expandiu suas operações, envolvendo-se também em atividades de ransomware, com vínculos a grupos como REvil e BlackMatter.
Essa evolução reflete uma mudança tática: além do roubo de dados, agora extorquem grandes somas em criptomoedas, ameaçando vazamento de informações.

O grupo é conhecido por sua organização profissional, empregando técnicas avançadas de engenharia social e infraestrutura de comando e controle sofisticada.
Mesmo após a prisão de alguns de seus membros, o FIN7 permanece uma ameaça significativa devido à sua capacidade de adaptação e resiliência, continuando a representar um perigo para o setor financeiro e outras indústrias globais.

A seguir, mencionamos algumas das principais vulnerabilidades identificadas como exploradas pelo grupo ou seus afiliados.

ID CVE	DESCRIÇÃO
CVE-2023-27532	Vulnerabilidade no componente Veeam Backup & Replication.
CVE-2021-34473	Vulnerabilidade de execução remota de código do Microsoft Exchange Server.
CVE-2021-34523	Vulnerabilidade de elevação de privilégio do Microsoft Exchange Server.
CVE-2021-31207	Vulnerabilidade de desvio de recurso de segurança do Microsoft Exchange Server.
CVE-2020-1472	Vulnerabilidade de elevação de privilégio no Netlogon (também conhecida como Zerologon).

Tabela 3 – Vulnerabilidades exploradas pelo FIN7.

3.4 Atores de estado-nação

3.4.1 Lazarus Group

O Lazarus Group, também conhecido como APT38, é um grupo avançado de ameaças persistentes (APT) ligado ao governo norte-coreano. Renomado por suas operações cibernéticas sofisticadas, o grupo realiza desde espionagem até ataques financeiros em larga escala. Sua principal meta é desviar grandes somas para financiar o regime norte-coreano.

Um dos ataques mais notórios do Lazarus ocorreu em 2016, quando tentou roubar 1 bilhão de dólares de uma instituição financeira, conseguindo transferir cerca de 81 milhões. O grupo usou técnicas avançadas, incluindo spear-phishing, malware personalizado e técnicas de "lateral movement" para alcançar seus objetivos.

Ao longo dos anos, o Lazarus tem evoluído, adotando novas técnicas e explorando vulnerabilidades emergentes. Sua adaptabilidade e complexidade operacional fazem dele uma das maiores ameaças cibernéticas globais, mantendo-se uma força ativa e perigosa no cenário cibernético.

Figura 5 – Fluxo de ataque Lazarus group.

A seguir, mencionamos algumas das principais vulnerabilidades identificadas como exploradas pelo grupo ou seus afiliados.

ID CVE	DESCRIÇÃO
CVE-2024-21338	Vulnerabilidade de elevação de privilégio do kernel do Windows.
CVE-2017-0199	Vulnerabilidade de execução remota de código do Microsoft Office/WordPad.
CVE-2020-1472	Vulnerabilidade de elevação de privilégio no Netlogon (também conhecida como Zerologon).
CVE-2023-42793	Bypass de autenticação ao RCE no JetBrains TeamCity.
CVE-2024-38193	Vulnerabilidade de elevação de privilégio do WinSock.

Tabela 4 – Vulnerabilidades exploradas pelo Lazarus group.

5 Soluções para sua segurança cibernética

Com a crescente digitalização dos serviços financeiros, o setor se tornou um alvo constante para cibercriminosos. Instituições enfrentam cada vez mais desafios de cibersegurança, exigindo cuidados ainda maiores com fraudes, inteligência artificial, deepfakes, entre outros crimes cibernéticos que podem impactar, ou até interromper completamente, as operações.

Nesse contexto, a aplicação de soluções do ISH Vision pode ser uma estratégia eficaz para mitigar ameaças cibernéticas.
Essa metodologia se divide em:

1. **GERENCIAMENTO DE DETECÇÃO E RESPOSTA (SIEM/MDR):** envolve a criação de uma visão de longo alcance do ambiente digital, com monitoramento contínuo e detecção avançada de ameaças. Ele detecta ataques antes que causem danos, investiga incidentes e aplica políticas personalizadas para fortalecer a segurança;

2. **DETECÇÃO E RESPOSTA EM ENDPOINTS (EDR):** fornece alta visibilidade em todos os endpoints do parque tecnológico, detectando ameaças potenciais por meio de machine learning e análise comportamental, oferecendo respostas a incidentes;

3. **DETECÇÃO E RESPOSTA EM REDES (NDR):** realiza a detecção no tráfego de rede com base na análise de protocolos e conteúdo transferido, extraindo arquivos de seções monitoradas.

O **Vision MEDR** se destaca como uma solução eficaz para fortalecer a segurança cibernética em ambientes complexos, como os do setor financeiro. Utilizando **inteligência artificial** de última geração, a plataforma detecta ataques desconhecidos e realiza a busca por ameaças de forma contínua e automatizada. Além disso, oferece funcionalidades, como:

1. **DETECÇÃO DE AMEAÇAS EM TEMPO REAL:**

   Utiliza ferramentas e técnicas avançadas para detectar ameaças em tempo real em todos os dispositivos endpoints da organização.

2. **RESPOSTA A INCIDENTES:**

   A solução responde a incidentes de segurança de forma rápida e eficaz para minimizar o impacto na organização.

3. **GESTÃO DE VULNERABILIDADES:**

   A solução responde a incidentes de segurança de forma rápida e eficaz para minimizar o impacto na organização.

4. **INVESTIGAÇÃO DE INCIDENTES:**

   Investiga os incidentes de segurança para determinar a causa e o impacto, e para recomendar medidas de resposta.

5. **RESPOSTA A INCIDENTES:**

   A solução responde a incidentes de segurança de forma rápida e eficaz para minimizar o impacto na organização.

6. **PROTEÇÃO CONTRA RANSOMWARE:**

   Oferece proteção contra ataques de ransomware, incluindo a detecção e bloqueio de ataques, a recuperação de dados criptografados e a contenção da propagação do ransomware.

7. **PROTEÇÃO CONTRA RANSOMWARE:**

   Identifica e corrige vulnerabilidades em endpoints.

8. **RELATÓRIOS E ANÁLISES:**

   Fornece relatórios e análises sobre as atividades de segurança e as ameaças detectadas.

6 Como manter sua organização protegida

Para aprimorar a maturidade de segurança no setor financeiro, recomendamos a implementação das seguintes medidas de proteção contra ransomwares, grupos APTs e malwares:

Autenticação Multifator (MFA): Implemente MFA para todos os serviços sempre que possível, com prioridade para e-mails, redes privadas virtuais (VPNs) e contas que acessam sistemas críticos.

Backups Regulares e Segregados: Realize backups frequentes de dados críticos, testando-os regularmente. Armazene-os fora do ambiente de produção e em locais segregados para garantir imunidade contra ataques de ransomware.

Atualizações e Patches: Mantenha todos os sistemas e softwares atualizados com os patches mais recentes, especialmente para sistemas comumente visados, como servidores de e-mail, sistemas de pagamento e dispositivos de rede.

Segmentação de Rede: Separe os segmentos de rede crítica para limitar a movimentação lateral de invasores. Utilize VLANs e firewalls internos para isolar sistemas sensíveis.

Monitoramento e Análise de Logs: Utilize ferramentas de SIEM (Security Information and Event Management) para monitorar e analisar logs de forma contínua, identificando e respondendo a atividades anômalas e tentativas de intrusão.

Treinamento de Funcionários: Eduque e treine continuamente os funcionários em práticas de segurança cibernética, phishing e engenharia social, destacando como evitar comprometimento de credenciais e a execução de arquivos maliciosos.

Controle de Acesso: Adote políticas de menor privilégio (Least Privilege) e controle de acesso baseado em funções (RBAC), garantindo que os usuários tenham acesso apenas ao necessário para suas funções.

Soluções de EDR: Implemente soluções de Endpoint Detection and Response (EDR) para monitorar e responder a atividades suspeitas nos endpoints, como tentativas de execução de ransomware.

Simulações de Ataque: Realize testes de penetração e exercícios de Red Team regularmente para identificar vulnerabilidades e avaliar a capacidade de resposta da organização.

Threat Intelligence: Utilize ferramentas de Threat Intelligence para monitorar e antecipar ameaças direcionadas ao setor financeiro, fornecendo informações valiosas sobre as táticas, técnicas e procedimentos (TTPs) utilizados por atacantes como o FIN7.

Políticas de Resposta a Incidentes: Desenvolva e mantenha políticas robustas de resposta a incidentes, incluindo planos de continuidade de negócios (BCP) e recuperação de desastres (DRP) específicos para ataques cibernéticos.

Criptografia de Dados Sensíveis: Assegure que todos os dados críticos, especialmente os relacionados a transações financeiras, estejam criptografados tanto em trânsito quanto em repouso.

Controle de Dispositivos Externos: Restrinja o uso de dispositivos externos, como pendrives e discos rígidos, e implemente soluções de Data Loss Prevention (DLP) para monitorar e controlar o fluxo de dados sensíveis.

Essas medidas, quando aplicadas em conjunto, aumentam significativamente a maturidade e resiliência das organizações financeiras contra os ataques cibernéticos atuais.

Protegendo o setor financeiro

Como vimos no decorrer deste e-book, a proteção do setor financeiro contra ameaças cibernéticas é crucial para garantir a continuidade dos serviços essenciais.

Ameaças como os ransomwares Black Basta e Qilin, além de malwares voltados para fraudes financeiras, como PixPirate, Mekotio e Grandoreiro, e grupos avançados como o FIN7 e o Lazarus, são apenas alguns exemplos do vasto leque de ameaças que podem impactar o setor.

Ataques de ransomware, como os do Black Basta e Qilin, podem causar interrupções significativas e exigir grandes somas em resgate. O grupo Lazarus, com suas técnicas avançadas de espionagem, roubo de dados e sabotagem, representa uma ameaça igualmente grave.

Por isso, é importante reconhecer que muitos outros atores, cada um com suas próprias táticas e objetivos, podem visar o setor. Se manter atualizado sobre novas ameaças e adotar uma abordagem abrangente e proativa são passos fundamentais para garantir a segurança e a continuidade das operações no setor financeiro.

AUTORES

Caique Barqueta
Especialista em Inteligência de Ameaças

Ismael Rocha
Analista de Inteligência de Ameaças Sênior

REFERÊNCIAS

Heimdall by ISH Tecnologia

A ISH pode ajudar a implementar a melhor estratégia de segurança cibernética para a sua empresa

Entre em contato com nosso time de especialistas e conheça as melhores soluções de cibersegurança do mercado

ISH | heimdall security research