Grupo Lazarus: Panorama das Ações Cibernéticas da Coreia do Norte

Anita Monteiro de Siqueira Pereira Bezerra, Jose Basilio da Silva Neto, Juan Felipe Serafim dos Santos, Maria Leticia Figueiroa Costa e Pedro Henrique Silva Durval dos Santos
E-mail(s): amspb@cin.ufpe.br, jbsn3@cin.ufpe.br, jfss@cin.ufpe.br, mlfc3@cin.ufpe.br, phsds@cin.ufpe.br

Resumo

O artigo analisa o *Lazarus Group*, grupo de cibercriminosos associado ao governo da Coreia do Norte, conhecido por ataques sofisticados com fins políticos e financeiros. Desde 2009, o grupo realiza operações globais, como o ataque à *Sony Pictures* e o *ransomware WannaCry*. Suas táticas incluem engenharia social, *spear phishing*, uso de malwares como *BlindingCan* e VHD, além de ataques distribuídos de negação de serviço (DDoS) e à cadeia de suprimentos. A Operação *DreamJob* exemplifica seu uso de falsas ofertas de emprego para comprometer sistemas. Os prejuízos ultrapassam bilhões de dólares, impactando criptomoedas, bancos e instituições públicas. O artigo destaca a importância de políticas robustas de segurança digital.
Palavras-chave: Ciberataques. Lazarus Group. Segurança cibernética.

Introdução

No universo da cibersegurança, existem grupos de Atores Estatais que são tipos de ameaças cibernéticas dirigidas e controladas por governos nacionais. Esses grupos, diferentemente de *hackers* comuns, têm objetivos alinhados aos interesses geopolíticos, econômicos e militares de seus países, como a prática de espionagem, roubo de informações confidenciais para beneficiar seu país, dentre outros fatores. A ascensão dos atores estatais na cibersegurança é uma das maiores preocupações globais, uma vez que têm a capacidade de causar danos massivos a toda a população, bem como têm a capacidade de fomentar guerras cibernéticas e instabilidades geopolíticas entre o mundo.

O *Lazarus Group* é um grande exemplo de ator estatal, visto que muitos acreditam, inclusive grandes Organizações como a *Federal Bureau of Investigation* (FBI), que o *Lazarus Group* é filiado e financiado pelo governo norte coreano e visa a proliferação de ataques cibernéticos por questões políticas econômicas, além de ter uma forte motivação financeira para apoiar o regime. Essa crença é corroborada pelo fato de que muitos de seus ataques e ameaças têm como alvo a Coreia do Sul e são realizados com o objetivo de espionar, perturbar e destruir essas redes. Tais ações visam tanto a coleta de informações sensíveis quanto a obtenção de recursos financeiros, que são direcionados ao financiamento dos programas militares e nucleares norte-coreanos. Além disso, o grupo busca desestabilizar adversários estrangeiros por meio de operações antiéticas e de impacto psicológico.

A Coreia do Norte passa a ser vista como a principal suspeita de direção do grupo, pelo agravante, também, de ser um dos países mais altamente desconectados da comunidade global, seja politicamente, tecnologicamente e economicamente. Portanto, devido à crise econômica norte-coreana, o regime encontrou uma forma de impulsionar suas questões financeiras e estratégicas.

Nesse cenário, cabe ressaltar que, na Coreia do Norte não existe internet livre, impossibilitando, assim, os hackers norte-coreanos de fazerem qualquer coisa por conta própria, sendo, portanto, necessário o apoio e treinamento do próprio governo. A *Kaspersky Lab*, empresa russa especializada na produção de softwares de segurança à internet, identificou múltiplos ataques desse grupo com o endereço de IP entre o *Bluenorff*, a China e a Coreia do Norte.

Também conhecido como APT38, uma entidade de Ameaça Persistente Avançada (APT), suas operações são bastante sofisticadas e geralmente envolvem a implementação de *malware* avançado, campanhas de *spear-phishing*, ataques de *watering hole*, invasões a *exchanges* de criptomoedas e a exploração de vulnerabilidades em sistemas.

Esse grupo de espionagem cibernética está ativo desde o ano de 2009 quando alguns sites dos Estados Unidos da América (USA) e da Coreia do Sul começaram a sofrer várias invasões de DDoS, dentre eles, alguns sites governamentais americanos, como o da Casa Branca, e alguns sites dos Ministérios Sul Coreanos. Ao longo dos anos o Grupo *Lazarus* conseguiu sofisticar as suas técnicas e aumentar suas escalas de operações cada vez mais, o que justificou o grande ataque à *Sony Pictures* no ano de 2014, às invasões aos bancos no Equador e Vietnã no ano de 2015, e ao banco do Bangladesh e Taiwan em 2016 e 2017, respectivamente.

Esses ataques de grande proporção permitiram uma maior visibilidade e destaque ao grupo, estabelecendo-os como uma forte ameaça significativa à segurança cibernética no mundo inteiro.

Esse mapa mostra, segundo os dados coletados pela ESET (uma empresa de segurança cibernética), o *Lazarus Group* agindo em nível mundial em diversas partes do globo.

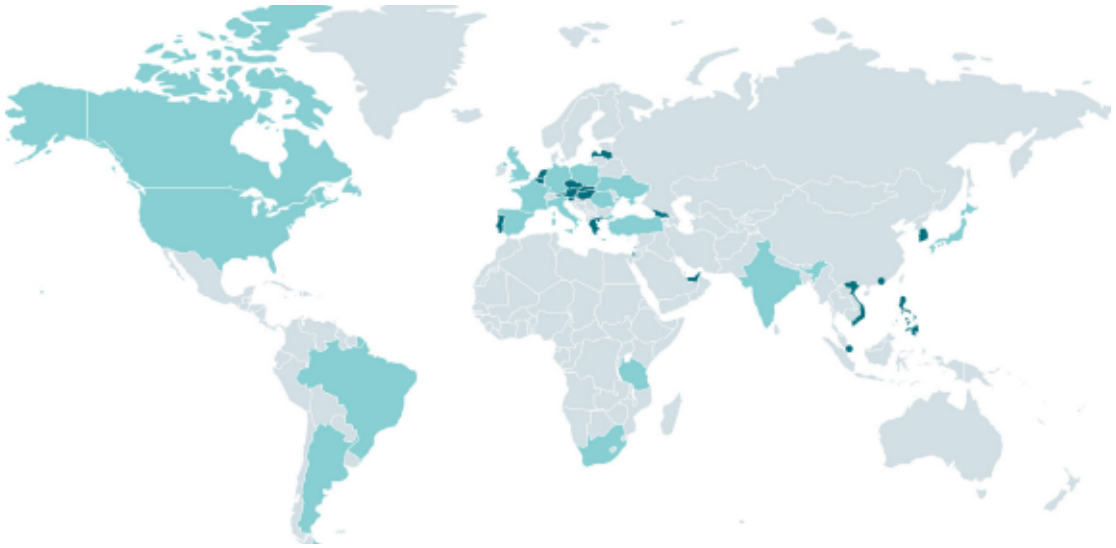

Figura 1: *Alvos registrados espalhados por todo o mundo (ESET, 2010)*

O Grupo *Lazarus* vem evoluindo suas táticas e técnicas ao longo dos anos de forma sofisticada e em grande escala. A cada novo ataque a bancos, corretoras de criptomoedas e instituições financeiras, mais difíceis as empresas de segurança têm de identificar e conter a ameaça cibernética. Ataques como *zero-day*, *Spear Phishing*, *Malware, Droppers, Backdoors* e dissimulação de informações enviesadas são exemplos de ameaças que vêm sendo desenvolvidas cada vez com mais técnica e qualidade.

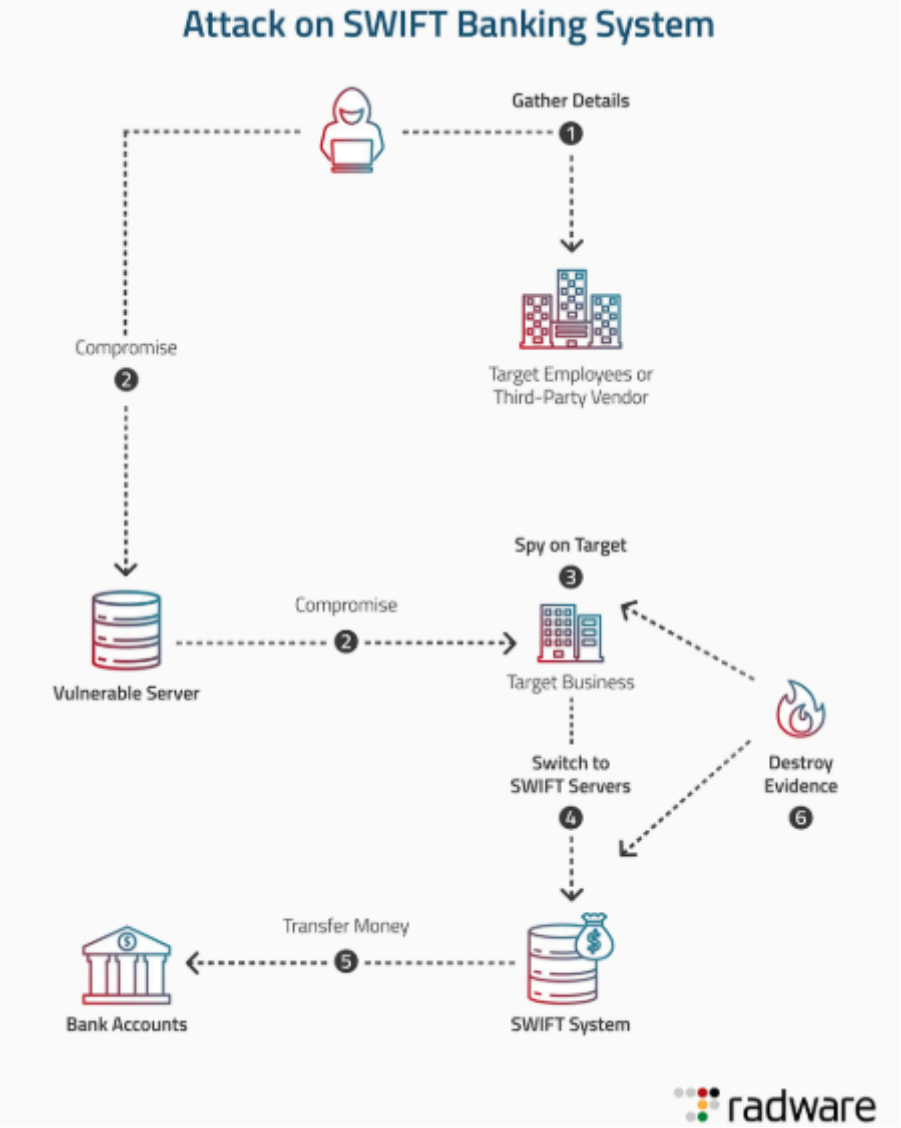

Figura 2: *Ataque ao sistema bancário SWIFT*

Diante dessa realidade, os profissionais de segurança e de tecnologia da informação de uma organização têm a responsabilidade de assegurar a proteção de toda a infraestrutura de rede contra diversas formas de ataque. Isso envolve manter todos os dispositivos conectados constantemente atualizados com os *patches* de segurança mais recentes, reduzindo ao máximo o risco de exploração de vulnerabilidades conhecidas. Ademais, considerando que o roubo de informações é um dos principais objetivos desses ataques, a proteção de dados sensíveis contra qualquer tipo de violação deve ser tratada como uma prioridade absoluta.

E isso mostra a importância e o objetivo deste *white paper* em evidenciar e esclarecer como esse grupo de *hackers* pode interferir no mundo e no atual cenário de segurança cibernética global. Diz respeito sobre um grupo muito sofisticado e poderoso patrocinado por um governo que opera no ciberespaço, escapando de sanções internacionais e usufruindo da tecnologia como uma arma geopolítica.

A partir disso, o estudo sobre as técnicas, os procedimentos e as táticas utilizadas pelo *Lazarus Group* é de extrema importância pois contribui diretamente para o aprimoramento de estratégias de defesa e de segurança cibernética. É a partir desse tema que pode ser instigado o debate sobre ciber conflitos e governança digital. Desse

modo, esse artigo reforça a importância de políticas de segurança mais robustas e na construção de estratégias que evitem casos de vulnerabilidades e ataques digitais.

Principais operações e ataques

Operação *DreamJob*

As campanhas atribuídas ao grupo *Lazarus* começaram a ser nomeadas formalmente a partir de 2020, embora evidências indiquem que suas atividades já ocorriam desde o início de 2009. Desde então, diversos incidentes foram reportados, muitos deles relacionados ao codinome *DeathNote* e caracterizados por ações direcionadas e persistentes. Um padrão recorrente observado nessas operações é o uso de softwares maliciosos disfarçados de ferramentas legítimas voltadas ao processo de recrutamento, como visualizadores de PDF, aplicativos de acesso remoto e desafios de programação. O principal malware utilizado nessas campanhas é o *BlindingCan*, um trojan de acesso remoto (RAT) que permite amplo controle sobre os sistemas comprometidos.

Além dele, outros *malwares* sofisticados também foram empregados, como o *ScoringMathTea* e o *LightlessCan*. O *ScoringMathTea* é uma *backdoor* avançada que disponibiliza 40 comandos, possibilitando a execução de tarefas como manipulação de arquivos, coleta de informações do sistema e execução de novos *payloads*, utilizando resolução dinâmica de APIs por meio de *hashes* personalizados. Já o *LightlessCan* representa um salto em furtividade: ele replica internamente comandos comuns do *Windows*, como *whoami, netstat e tasklist*, evitando que sejam executados diretamente no terminal, o que dificulta sua detecção por soluções de segurança comportamentais, como Detecção e Resposta em Endpoints.

A Tabela 1 resume os ataques da Operação *DreamJob* observados pela ESET e no *VirusTotal* desde o final de 2021. Ela mostra o tipo de interface entregue à vítima (quando existente) e a marca falsamente representada pelos atacantes.

Data	País	Tema	Indústria	Cargas
2021-09	Bélgica	Amazon	Mídia	OfficeCertTea
2021-10	Países Baixos	Amazon	Aeroespacial	BlindingCan, FudModule, HTTP(S) uploader
2022-03	Espanha	Desafios de programação + Meta	Aeroespacial	BlindingCan, miniBlindingCan, LightlessCan, NickelLoader
2022-03	África do Sul	SecurePDF + Airbus		ImprudentCook
2023-01	India	SecurePDF + UltraVNC + Accenture	Tech & Data	miniBlindingCan, BlindingCan, LightlessCan
2023-02	*	Comcast		miniBlindingCan
2023-03	Georgia	HSBC		SimpleTea for Linux
2023-05	Hungary	TightVNC + Rosatom		WinInetLoader

***Tabela 1**: Instâncias da operação DreamJob desde 2021.*

Ciberataques e criptomoedas

O *Lazarus Group*, têm sido os *hackers* de criptomoeda mais ativos nos últimos anos. Em 2022, quebraram seus próprios recordes de roubo, roubando cerca de US$1,7 bilhão em criptomoedas por meio de vários ataques, por exemplo, o *WannaCry*. Para contextualizar, as exportações totais da Coreia do Norte em 2020 totalizaram 142 milhões de dólares em bens, a maioria dos especialistas concorda que o governo norte-coreano está utilizando os bens roubados para financiar os programas de armamento nuclear.

Em maio de 2017, o grupo *Lazarus* esteve por trás da propagação do *ransomware WannaCry*, que encripta arquivos de vítimas ao redor do mundo e exige um resgate entre US$300 e US$600 em bitcoins para a liberação dos dados. Estima-se que os invasores tenham arrecadado aproximadamente US$150 mil em bitcoins nos meses seguintes ao ataque. O *WannaCry* atingiu mais de 200 mil computadores em 150 países, causando danos que variam entre centenas de milhões e bilhões de dólares. No Reino Unido, o Serviço Nacional de Saúde (NHS) foi particularmente afetado, com departamentos de emergência paralisados e consultas urgentes remarcadas, resultando em prejuízos estimados em cerca de £ 5,9 milhões.

O ataque à *Sony Pictures*, realizado pelo grupo autodenominado "Guardiões da Paz" — posteriormente identificado como parte do grupo *Lazarus* — causou danos avaliados em aproximadamente US$15 milhões, cobertos pelo seguro da empresa. Estimativas externas apontam para custos de recuperação entre US$35 milhões e mais de US$85 milhões, além dos significativos danos à reputação da companhia. Os *hackers* teriam tido acesso aos sistemas da *Sony* por mais de um ano antes do ataque, durante o qual grandes volumes de dados foram roubados e divulgados gradualmente. Entre os materiais comprometidos estavam filmes inéditos, e-mails corporativos e informações pessoais de milhares de funcionários.

O propósito real do ataque ainda é alvo de especulação. Uma possível motivação seria a retaliação à *Sony* pela produção de um filme que retratava o líder norte-coreano de forma desfavorável, o que teria desagradado o governo da Coreia do Norte. Os "Guardiões da Paz" chegaram a ameaçar medidas severas contra quem assistisse ao filme. Embora o governo norte-coreano tenha negado envolvimento direto, suspeitas indicam que o ataque pode ter sido orquestrado por hackers a serviço do regime, com algumas teorias sugerindo inclusive a participação de *hackers* russos alinhados politicamente.

Técnicas, Táticas e Procedimentos (TTPs)

O *Lazarus Group*, associado ao regime norte-coreano, se consolidou como uma das ameaças cibernéticas mais sofisticadas e persistentes da atualidade. Seu sucesso se deve a um conjunto bem estruturado de técnicas, táticas e procedimentos, cuidadosamente combinados para alcançar objetivos que vão desde espionagem até extorsão financeira. As campanhas do grupo são executadas em estágios, integrando ataques técnicos com exploração humana e de vulnerabilidades tecnológicas, sempre com alto grau de planejamento estratégico.

Engenharia Social: o ponto de entrada

Grande parte das operações do grupo *Lazarus* começa com a engenharia social, especialmente por meio de *spear phishing*, que são e-mails personalizados com anexos ou links maliciosos. Esses e-mails se disfarçam de comunicações legítimas, como

ofertas de emprego ou documentos internos, e são capazes de enganar até usuários experientes. Foi por meio dessa tática que o grupo conseguiu invadir a *Sony Pictures*, em um ataque que causou grandes prejuízos financeiros e à reputação da empresa.

Além de enganar usuários, o grupo também aplica técnicas de guerra psicológica, como campanhas de bandeira falsa, que tentam mascarar a origem real dos ataques e confundir os esforços de resposta. Esse componente psicológico dos ataques revela uma consciência geopolítica e uma intenção deliberada de manipular não apenas sistemas, mas também a percepção das vítimas.

Um exemplo relevante é a Operação *DreamJob*, na qual o grupo *Lazarus* explorou plataformas como o LinkedIn para enganar funcionários de empresas de tecnologia e defesa com falsas ofertas de trabalho. Após abrir arquivos maliciosos, as vítimas tinham seus sistemas comprometidos, o que permitia a instalação de malware e roubo de dados, incluindo no caso do assalto à *exchange* Indodax.

Implantação de malware: escalada e persistência

Com o acesso inicial garantido, o grupo avança utilizando malwares personalizados. Essas ferramentas variam de acordo com o objetivo da campanha: desde *trojans* de acesso remoto e *wipers* destrutivos até *ransomwares* como o VHD, projetado para criptografar dados e exigir resgate.

O grupo *Lazarus* se destaca também por empregar ataques de *watering hole*, nos quais sites legítimos são comprometidos para infectar visitantes específicos e pela exploração de vulnerabilidades de dia zero, ou seja, falhas ainda desconhecidas pelos fabricantes de software.

Entre as famílias de *malware* mais conhecidas estão o *Castov*, usado para roubo de credenciais e abertura de *backdoors*, e o *Destover*, um *malware* destrutivo que elimina arquivos e dificulta a recuperação dos sistemas afetados. Essas ferramentas permitem ao grupo manter acesso contínuo e discreto aos sistemas infectados, mesmo após tentativas de limpeza.

Além disso, o grupo realiza ataques à cadeia de suprimentos, introduzindo código malicioso em bibliotecas e *softwares* de código aberto amplamente utilizados. Isso amplia o alcance dos ataques, permitindo atingir diversas empresas por meio de um único ponto comprometido.

Sabotagem e interrupção: o uso tático de DDoS

Em suas operações mais agressivas, o *Lazarus Group* lança ataques DDoS para tirar serviços do ar ou desviar a atenção das equipes de segurança. Ao sobrecarregar redes e servidores com tráfego falso, o grupo cria brechas temporárias para atividades paralelas, como exfiltração de dados ou inserção de novos *malwares*.

Para esses ataques, o grupo frequentemente utiliza dispositivos IoT comprometidos, ampliando seu poder de fogo e aumentando a dificuldade de rastreamento. A coordenação desses ataques evidencia a capacidade técnica do grupo de causar interrupções massivas em serviços governamentais, financeiros e de infraestrutura crítica.

Evasão e anti-forense: escondendo rastros

Outro ponto de destaque na atuação do grupo *Lazarus* é sua habilidade em evitar detecção e apagar rastros. O grupo utiliza ferramentas legítimas do sistema operacional, como msmpeng.exe e bitsran.exe, para executar ações maliciosas sem levantar suspeitas. Além disso, adota técnicas anti-forenses, como a exclusão de *logs*, uso de criptografia e limpadores de disco, dificultando análises pós-incidente e atrasando as respostas das equipes de segurança.

Essas táticas revelam um entendimento profundo das ferramentas de detecção e das rotinas de investigação digital, reforçando o perfil de um ator altamente preparado e focado na permanência e no sigilo.

Espionagem e exfiltração: o objetivo final

Em muitos casos, o objetivo final das campanhas é a espionagem cibernética. Após obter acesso prolongado aos sistemas, o grupo realiza a exfiltração de dados sensíveis, como documentos financeiros, industriais, governamentais ou militares. Essas informações são utilizadas para fins estratégicos ou monetizados em mercados clandestinos.

O grupo *Lazarus* também se aproveita de sistemas de pagamento, plataformas de criptomoedas e redes financeiras como o SWIFT, demonstrando seu foco em alvos que vão além da espionagem tradicional e incluem ganho financeiro direto.

Ferramentas e Malwares utilizados

Além das táticas e técnicas apresentadas, o Grupo Lázaro também se faz de outras ferramentas para seus ataques, como o uso de diferentes *malwares*, demonstrando a sua natureza de atacar diretamente a segurança cibernética e o aproveitamento de vulnerabilidades presentes nos sistemas das vítimas. Dentre os *malwares* utilizados, destacam-se:

- ***WannaCry*:** O ataque mais conhecido realizado pelo grupo, o malware foi disseminado por meio de um *exploit* chamado "*EternalBlue"* que se aproveitava de uma falha de sistema presente em diversos dispositivos usuários do sistema operacional *Windows*, dispositivos esses que não possuíam o último *patch* para correção de *exploits* lançados há 2 meses antes dos ataques. O *WannaCry* é um *ransomware* de criptografia cujo objetivo de sua utilização é extorquir dinheiro, criptografando os arquivos de um usuário e impossibilitando seu uso ou controle de acesso do computador da vítima.

- ***Castov*:** O *Castov* foi utilizado pelo grupo *Lazarus* para atacar instituições financeiras sul-coreanas e seus clientes durante o início do ano de 2013, resultando em um massivo roubo de dados como senhas, detalhes de contas e certificados digitais, com o *malware* também sendo utilizado posteriormente em outros ataques de DDoS contra outras instituições sul-coreanas em junho do mesmo ano.

- ***Destover*:** Ocorrendo por volta do ano de 2014, o *malware* foi capaz de afetar o próprio disco rígido do computador das vítimas impossibilitando o seu uso, além de fornecer acesso a arquivos pessoais, destacando-se como ataque mais famoso do grupo o realizado contra a empresa "*Sony Pictures*". Durante o ataque, o grupo de *Hackers* teve acesso a diversas pastas que continham senhas e informações privadas da empresa, como dados dos funcionários e até mesmo e-mails pessoais com mensagens de dentro e fora da organização.

- ***Virtual Hard Disk* (VHD):** O VHD (Disco rígido virtual) é uma ferramenta de *ransomware* que busca infiltra-se nas unidades conectadas ao computador da vítima, criptografando seus arquivos e excluindo todas as pastas que possam auxiliar na recuperação do sistema, além de impossibilitar a proteção de arquivos importantes que possuem sistemas de segurança contra modificações.
  Para o ataque, o *ransomware* possuía um acesso prévio a listas de endereços IP dos computadores da vítima por meio de uma vulnerabilidade presente em sistemas de VPN, como também as credenciais das contas das vítimas que lhe garantiam direitos de administrador, cujo foram utilizadas para a realização de ataques de força bruta ao serviço SMB. Caso o *malware* conseguisse se conectar usando o protocolo SMB ao sistema, o mesmo se clonaria e se auto executava criptografando a máquina, assim ocasionando no seu bloqueio ao acesso pelo usuário.

- ***Fallchill*:** Dentre as ferramentas utilizadas pelo grupo Lázaro, o *trojan Fallchill* é responsável por criar uma *Backdoor* dentro de um sistema viabilizando ataques de outros invasores ou malwares. O ataque começou quando um funcionário da organização *exchange* recebeu uma oferta por email de um aplicativo de operações financeiras, compra e venda de moedas virtuais denominado "*Celas Trade Pro*", disponibilizado pela *Celas Limited*. Embora tenham sido apresentados certificados oficiais de confiabilidade SSL, ao se iniciar uma atualização do sistema, o dispositivo acabou por permitir a entrada de um *trojan* de *backdoor*. O grupo de cibercriminosos utilizaram desse *backdoor* para ter acesso a diversas funcionalidades presentes nos sistemas infectados, dentre elas administrar arquivos do servidor de comando, gravar dados em um arquivo específico, apagar arquivos, e por fim baixar e executar ferramentas adicionais.

- ***Brambul*:** O *Brambul* é um ransomware do tipo worm focado em Server *Message Block* (SMB) para *Windows* de 32 bits, funcionando como um arquivo de biblioteca de vínculo dinâmico (DLL) como um arquivo executável portátil, frequentemente baixado e instalado na rede das vítimas por um *malware dropper*. O *Server Message Block* (SMB) é um método usado pelos sistemas *Microsoft* para compartilhar arquivos em uma rede, sendo nesse contexto que o *Brambul* quando executado procura estabelecer um contato com os sistemas das vítimas e endereços IP nas sub-redes locais das vítimas. Seu objetivo é se espalhar entre contas de usuários desprotegidos e obter acesso não autorizado por meio do protocolo SMB (portas 139 e 445), lançando ataques de força bruta para obtenção de senhas usando uma lista de senhas incorporadas, além de comunicar informações sobre o sistema das vítimas.

Impactos e Repercussões

Os danos causados pelos cibercriminosos em suas vítimas variam entre corrupção e perda total de dados, prejuízo fortemente financeiro, como também o temor e receio de que informações privadas sejam novamente divulgadas sem a devida permissão.
Como dito anteriormente, eles são caracterizados como Ameaças **Persistentes** Avançadas e portanto, algumas campanhas duram cerca de meses a anos de atividade, o que culmina em um impacto considerável ao alvo afligido.

Impactos financeiros

Para as campanhas relacionadas a roubos de carteira de criptomoedas, como o caso mais recente da empresa *ByBit*, o prejuízo estimado ultrapassa os $1,4 bilhão de dólares (aproximadamente R$8,7 bilhões na cotação de quando aconteceu o roubo). De acordo com o CEO da *ByBit*, esse foi um caso isolado e direcionado especificamente para uma única carteira digital.

A repercussão da notícia desvalorizou as ações das principais criptomoedas atuais, como o *Bitcoin* que recuou em mais de 1,5% e o *Etherium* (principal moeda roubada no hack) em mais de 2%.

Outro caso financeiro notório ocorreu com o Banco Central de *Bangladesh*, em que $81 milhões de dólares foram efetivamente roubados do *Federal Reserve Bank of New York*. O grupo explorou a vulnerabilidade humana através de Engenharia Social para infectar o computador de um dos funcionários do banco, em seguida contaminou a rede interna do banco para então, de maneira simplificada, encontrar credenciais válidas para autorizar a transferência e esconder os rastros.

Além do prejuízo monetário, a confiança sobre instituições bancárias que utilizam o *Swift* foi abalada, pois mesmo que a rede *Swift* não tenha sido invadida ou adulterada, o fato de ter ocorrido um ataque em um banco que se utiliza dessa rede, contribui para uma sensação de insegurança por parte dos clientes.

Impactos institucionais

Com a campanha que culminou no uso do *ransomware WannaCry*, cerca de 250.000 computadores em 150 países foram afetados com a encriptação de informações salvas, cuja consequência se deu pela perda total de dados ou pagamento com o objetivo de recuperar as informações mas sem garantia de decriptação dos dados.

O *ransomware* repercutiu fortemente no ambiente empresarial, obrigando as empresas a no mínimo atualizarem o sistema operacional (S.O) das máquinas para uma versão *patcheada*, cuja vulnerabilidade conhecida como *EternalBlue* não existisse para evitar a disseminação do ransomware via rede interna da empresa em questão.
Mas o dano não foi somente no contexto empresarial. A *National Health Service* (NHS) do Reino Unido não pôde funcionar, paralisando atendimento de saúde ao público e suspendendo cirurgias.
Outras instituições suspenderam suas atividades até ter quase todos os computadores atualizados. Muitas destas ainda utilizavam o S.O *Windows XP* que é vulnerável ao *EternalBlue*.

Respostas Internacionais e Medidas de Mitigação

As autoridades dos países que foram alvos e vítimas dos ataques do grupo Lazarus reagem, principalmente - diante de indícios do grupo ser ligado ao governo norte coreano -, com sanções políticas e econômicas. O Departamento do Tesouro dos EUA, por exemplo, aplicou pela primeira vez sanções a um misturador de moedas virtuais, o *Blender.io*, por facilitar a lavagem de dinheiro de crimes cibernéticos vinculados à Coreia do Norte, enquanto que a União Europeia sancionou a empresa *Chosun Expo* por apoiar o grupo *Lazarus* em suas campanhas que resultaram no roubo ao Banco de *Bangladesh* e ao ataque à *Sony Pictures Entertainment*.
Essas sanções incluem congelamento de bens, proibição de viagens e impedimentos legais para indivíduos e empresas da União Europeia que forneçam recursos financeiros aos sancionados.

Diante disso, considerando as TTP's utilizadas pelo grupo *Lazarus*, maneiras de mitigar tais incidentes seriam as seguintes:

1. **Uso de protocolos de autenticação de e-mail pelo servidor de e-mail**: o uso de protocolos como o SPF, DKIM e DMARC pelo servidor de e-mail da organização contribui para evitar uma abordagem oportunista por e-mail.
2. **Treinamento e conscientização de funcionários**: treinamentos regulares com todos os colaboradores sobre os potenciais riscos de ataques direcionados de *phishing*.
3. **Realização de *backups* regulares além de *backups offline***: realizar *backups* frequentemente reduz o impacto de um ataque de *malware* e/ou *ransomware,* pois as informações significantes estarão a salvo da infecção. Além disso, fazer um *backup offline* evita uma potencial infecção das informações salvas, pois pode vir a existir a possibilidade do *malware* se infiltrar entre a cópia de segurança e comprometê-la.
4. **Filtro de arquivos esperados a serem recebidos e inspecione regularmente o que for recebido**: caso seja necessário receptar algum arquivo de alguma origem conhecida, adicionar um filtro com a extensão do arquivo esperado e investigar se tal arquivo é seguro por meio de *antimalware*.
5. **Manter *antimalware* e outros softwares utilizados no ambiente organizacional sempre atualizados**: deixar o sistema "em dia" evita que seja explorada alguma vulnerabilidade ainda não descoberta em algum software empresarial ou pessoal.
6. Para ataques DDoS existem pelo menos **quatro** estágios de mitigação:
    a. **Detecção**: utilização de um *Intrusion Prevention System* (IPS) para impedir tentativas de conexão fora do comum além de outras abordagens para distinguir uma tentativa efetiva de ataque.
    b. **Resposta**: após identificar a ação de ataque, utilizar-se de recursos para impedir a perpetuação e continuação do ataque.
    c. **Roteamento**: identificando corretamente os agentes atacantes, dividir o tráfego em blocos, de tal maneira gerenciáveis manter o acesso a aplicação perene.
    d. **Adaptação**: analisar padrões de acesso à aplicação, considerando a origem da conexão e os blocos de IPs maliciosos conhecidos, e bloquear tentativas anômalas de acesso.
7. **Análise de *logs***: o gerenciamento de informações e eventos de segurança (SIEM) serve exatamente para esse fim, concentrando informações de diversas fontes e entregando com clareza imediata sobre o comportamento dos dispositivos, acessos e incidentes correlatos à segurança.

Como o grupo tem evoluído ao longo dos anos?

Desde os primeiros registros de suas campanhas, sendo essa primeira conhecida como *Operation Troy* cuja especialidade inicial foi um ataque (DDoS) sobre as forças armadas sul coreanas, o grupo tem progredido em suas TTP's de maneira agressiva, diversificando sua variedade de ataques utilizados, de alvos a serem espionados e atacados e cada vez mais explorando novas possibilidades e vulnerabilidades existentes ou (até então) não conhecidas ao público.
É espantoso como determinadas campanhas escalam e como técnicas de intrusão, antes impensáveis, são postas em prática e concretizadas para atingir seus objetivos.

Ao longo de toda essa trajetória, alguns elementos permanecem constantes: o alto grau de planejamento, a integração com os interesses estratégicos do regime norte-coreano e a rápida capacidade de adaptação diante de sanções ou interrupções operacionais. O grupo *Lazarus* representa, assim, não apenas uma ameaça cibernética persistente, mas também um caso emblemático de como grupos patrocinados por governos podem operar na fronteira entre ciberespionagem, cibercrime e guerra cibernética, com impacto global.

Considerações finais

A capacidade do Lazarus Group de combinar engenharia social, *malware* sob medida, ataques à cadeia de suprimentos, movimentações laterais, sabotagem, técnicas anti-forenses e espionagem cibernética demonstra uma abordagem modular, adaptável e altamente estratégica. Seus ataques não são isolados ou improvisados, mas sim parte de campanhas bem planejadas, que operam com o profissionalismo e os recursos típicos de um ator patrocinado por um governo.

Essa atuação coloca o grupo entre as ameaças mais complexas da cibersegurança contemporânea, com impacto direto na estabilidade de sistemas financeiros, infraestruturas críticas e segurança da informação em escala global. Suas operações comprometem diretamente não apenas empresas, mas a estabilidade digital de governos inteiros, tornando essencial o estudo contínuo de suas TTPs para fortalecer defesas cibernéticas no mundo todo.

Bibliografia Consultada

NCC Group. The Lazarus Group: North Korean scourge for plus 10 years. NCC Group, [s.l.], [s.d.]. Disponível em: https://www.nccgroup.com/us/the-lazarus-group-north-korean-scourge-for-plus10-years/. Acesso em: 1 jul. 2025.

PANKOV, Nikolay. Lazarus experiments with new ransomware. Kaspersky Blog, 2020. Disponível em: https://www.kaspersky.com/blog/lazarus-vhd-ransomware/36559/. Acesso em: 30 jun. 2025.

GRUSTNIY, Leonid. Hackers da Coreia do Norte criam software para roubar criptomoedas. Kaspersky Brasil Blog, 2018. Disponível em: https://www.kaspersky.com.br/blog/lazarus-crypto-exchange-attack/10793/. Acesso em: 30 jun. 2025.

GULYÁS, Attila. "LAZARUS" The North Korean Hacker Group. In: STRATEGIES XXI – The Complex and Dynamic Nature of the Security Environment. Disponível em: https://www.researchgate.net/publication/358531629_LAZARUS_THE_NORTH_KOREAN_HACKER_GROUP. Acesso em: 3 jul. 2025.

PALANIAPPAN, Gopinath et al. An Intrusion Using Malware and DDNS. arXiv preprint, 2019. Disponível em: https://arxiv.org/pdf/1902.09158. Acesso em: 30 jun. 2025.

KÁLNAI, Peter. Lazarus campaigns and backdoors in 2022–2023. Czechia: ESET, 2023. Disponível em: https://www.researchgate.net/publication/374977618_Lazarus_campaigns_and_backdoors_in_2022-2023. Acesso em: 4 jul. 2025.

Thread Intel, Symantec. Lazarus: History of mysterious group behind infamous cyber attacks. Medium, [s.l.], [s.d.]. Disponível em: https://medium.com/threat-intel/lazarus-attacks-wannacry-5fdeddee476c. Acesso em: 29 jun. 2025.

Arif Perdana et al. Hack, heist, and havoc: The Lazarus Group's triple threat to global cybersecurity. SAGE Journals, 2024. Disponível em: https://journals.sagepub.com/doi/epdf/10.1177/20438869241303941. Acesso em: 30 jun. 2025.

U.S. Department of the Treasury. U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats. U.S. Treasury, [s.l.], 2022. Disponível em: https://home.treasury.gov/news/press-releases/jy0768. Acesso em: 1 jul. 2025.

The New York Times. The Billion-Dollar Bank Job. 2018. Disponível em: https://www.nytimes.com/interactive/2018/05/03/magazine/money-issue-bangladesh-billion-dollar-bank-heist.html. Acesso em: 2 jul. 2025.

Kaspersky Resource Center, [s.l.], [s.d.]. Ransomware WannaCry: tudo o que você precisa saber. Disponível em: https://www.kaspersky.com.br/resource-center/threats/ransomware-wannacry. Acesso em: 2 jul. 2025.

SegInfo. Dicas de mitigação de ataques de malware e ransomware., 22 ago. 2022. Disponível em: https://seginfo.com.br/2022/08/22/dicas-de-mitigacao-de-ataques-de-malware-e-ransomware/. Acesso em: 2 jul. 2025.

Lawfare Media. Countering North Korean Cybercrime and its Enablers. Disponível em: https://www.lawfaremedia.org/article/countering-north-korean-cybercrime-and-its-enablers. Acesso em: 30 jun. 2025.

Times of Malta. BOV hacker links to North Korea exposed in new BBC podcast. Disponível em: https://timesofmalta.com/article/bov-hacker-links-north-korea-exposed-new-bbc-podcast.1025564. Acesso em: 30 jun. 2025.

KÁLNAI, Peter. Lazarus Group: A mahjong game played with different sets of tiles. Disponível em: https://www.researchgate.net/profile/Peter-Kalnai/publication/335219752_Lazarus_Group_a_mahjong_game_played_with_different_sets_of_tiles/links/5d7949ed299bf1cb8099710f/Lazarus-Group-a-mahjong-game-played-with-different-sets-of-tiles.pdf. Acesso em: 30 jun. 2025.

Alex O'Neill. Countering North Korean Cybercrime and its Enablers. Disponível em: https://www.lawfaremedia.org/article/countering-north-korean-cybercrime-and-its-enablers. Acesso em: 30 jun. 2025.

BOV hacker links to North Korea exposed in new BBC podcast. Disponível em: https://timesofmalta.com/article/bov-hacker-links-north-korea-exposed-new-bbc-podcast.1025564. Acesso em: 30 jun. 2025.