

**ASSOCIAÇÃO DE ENSINO E CULTURA DE MATO GROSSO DO SUL – FACULDADES INTEGRADAS**

**TECNÓLOGO EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS**

**SEGURANÇA DA INFORMAÇÃO**

ALUNO: Wellington Aparecido Afonso Da Silva

Análise e Desenvolvimento De Sistemas Faculdades Integradas De Três Lagoas

[Wellingtoon20021@gmail.com](mailto:Wellingtoon20021@gmail.com)

Professor: Richard Vieira Do Espirito Santo.

Docente das Faculdades Integradas De Três Lagoas

**TRÊS LAGOAS**

**19/03/2024**

# **RESUMO**

Carbanak é um grupo cibercriminoso conhecido em todo o mundo por seus ataques sofisticados de hackers e instituições financeiras. Originário da Europa de Leste, este grupo é famoso pelos seus ataques cibernéticos que visam roubar grandes quantidades de dinheiro de bancos e outras instituições financeiras em todo o mundo. Usando malware avançado e engenharia social, Carbanak conseguiu penetrar em sistemas altamente seguros, comprometer redes bancárias e transferir fundos ilegalmente. Suas ações causaram perdas significativas a diversas instituições financeiras e causaram preocupação generalizada na indústria de segurança cibernética. Carbanak representa uma ameaça contínua à segurança financeira global, exigindo uma resposta colectiva e vigilância constante por parte das agências e organizações relevantes

Sumário

[**RESUMO** 2](#_Toc161561465)

[**Objetivos** 4](#_Toc161561466)

[PHISHING ATACK 4](#_Toc161561467)

[**O CARBANAK** 5](#_Toc161561468)

[Como Começou? 5](#_Toc161561469)

[**REDE SWIFT** 5](#_Toc161561470)

[Oque é? 5](#_Toc161561471)

[**O QUE VEM POR AI?** 6](#_Toc161561472)

[Europol 7](#_Toc161561473)

[TAIWAN 2016 7](#_Toc161561474)

[ESPANHA 2018 8](#_Toc161561475)

[**REFERÊNCIAS BIBLIOGRÁFICAS** 10](#_Toc161561476)

# **Objetivos**

Esta pesquisa tem como objetivo relatar os ataques feitos por hackers em bancos. Conhecido como **CARBANAK** O mais completo e perigoso pertencente ao grupo de crimes cibernéticos do tipo APT**,** para comprometer bancos os invasores enviaram e-mails(PHISHING) de origem maliciosas para funcionários de instituições bancárias que infectaram máquinas com malware quando abertos. E assim conseguiam fazer transferências bancárias para caixas eletrônicos que eles faziam monitoramento e assim conseguiam resgatar o dinheiro.

## PHISHING ATACK

Neste tipo de ataque os hackers tentam se parecer o mais verdadeiro possível, criando e-mails que se passam por pessoas ou empresas reais. Esses e-mails podem ter arquivos com extensão de WORD, EXECEL OU POWER POINT ou até mesmo imagens e vídeos que uma vez executado os criminosos conseguem vigiar e controlar a máquina, consequentemente eles usam essa máquina infectada para infectar outros computadores conectado a mesma rede

Texto sobre foto de mulher

Descrição gerada automaticamente com confiança média

# **O CARBANAK**

## Como Começou?

Descoberto em 2014 por pesquisadores da KASPERSKY LAB, que investigavam fraudes de roubos em caixas eletrônicos, investigadores iniciaram uma investigação sobre roubos de caixas eletrônicos, mas rapidamente encontraram evidências de que esses incidentes estavam relacionados e faziam parte de uma grande operação internacional para roubar grandes somas de dinheiro de vários bancos de mercadorias no mundo. Nas primeiras abordagens foram investigados somente países da Europa Ocidental, por consequência acabaram encontrando mais vítimas na China, Alemanha e Estados Unidos.

Os Hackers usavam dessemelhantes formas para conseguirem chegar ao dinheiro. Como tinham controle total remotamente dos caixas eletrônicos eles davam as instruções a esses caixas e mais tarde as “mulas” como eram conhecidos, passavam recolhendo os malotes. Em outros cenários usavam a rede **SWIFT** usada para transferência diretas para suas contas. Até o ano de 2014, esse modo era tratado como novidade já que ninguém nunca usado para este tipo de operação, de modo que as tecnologias usadas pelo grupo deixaram o setor bancário e da cibersegurança em choque.

# **REDE SWIFT**

## Oque é?

Denominado como um código universal com oito caracteres que identifica a instituição bancária durante o processo de transferência de dinheiro entre países, onde os primeiros quatro caracteres identificam o código do banco, os outros dois vão identificar o país e os outros dois irão identificar a cidade. Fundada em 1973 pelos americanos e europeus para fins de transições interbancárias e atualmente possui um pouco mais de 11 milhões de instituições financeira espalhas por mais de 200 países.

# **O QUE VEM POR AI?**

Após descoberta do carbanak. Investigadores obtiveram contato com vários ataques que tentaram táticas idênticas, mas agora que o código-fonte acesso público, tipo de incidentes como esse podem acontecer com mais frequência já que está disponível para criminosos que não tem tanta experiencias em codificação para produzir malware complexos.  **O** **ESPECIALISTA DA KASPERSKY LAB SERGEY GOLOVANOV**  tem uma fala sobre isso:

*“O fato de o código-fonte do famoso malware* [*Carbanak*](https://securelist.com/the-great-bank-robbery-the-carbanak-apt/68732/) *estar disponível em um site de código aberto é um mau presságio. Na verdade, o Carbanak foi desenvolvido com o código-fonte do malware Carberp após sua publicação online. Temos razões para acreditar que esta situação se repetirá e que veremos modificações mais perigosas no futuro. A boa notícia é que, desde o vazamento do Carberp, a indústria de segurança cibernética evoluiu significativamente e o código modificado agora pode ser facilmente detectado. Por isso, incentivamos empresas e usuários individuais a se protegerem contra essas ameaças e contra aquelas que ainda nem existem por meio de uma solução de segurança confiável. ”*

## Europol

Um funcionário da Kaspersky Lab descobriu uma fragilidade no código da carbanak. Esse erro permitiu que especialistas enviassem uma solicitação aos servidores de comando e controle da carbanak, de forma simples se eles enviassem uma mensagem muito especifica a esse servidor eles iriam receber uma resposta muito especifica, no entanto ninguém sabia o endereço físico e nem digital desse servidor como solução os agentes fizeram uma varredura em toda internet e foram distribuindo essa solicitação a cada servidor conectado a web, e assim ficaram aguardando resposta de algum deles.

Após dois dias conseguiram uma resposta que veio de um país com a maior infraestrutura de T.I da Europa e o segundo com maior conectividade no mundo a Holanda, rapidamente conseguiram acesso a máquina e chamou os especialistas para checarem e com isso teve uma descoberta ao escopo que causou espanto a todos, já tinha ataques espalhados por todos os países ao redor do mundo, um valor próximo a 700.000.000 milhões de dólares foram roubados sigilosamente.

## TAIWAN 2016

Depois de incidente os hackers ficaram cerca de 6 meses em silencio e voltaram fazendo o maior erro de suas carreiras, foi em Taiwan que a descoberta começou a ser feita. Após tentaram saquear dinheiro de alguns caixas eletrônicos que estavam sendo hackeados, duas “mulas” acabaram cometendo um grande erro e deixaram cerca 60.000,00 mil dólares no caixa eletrônico, pelo fato de ter aproximado uma pessoa desconhecida que possivelmente queria usar o caixa eletrônico de forma legal. Surpreso com a situação de terem deixado um valor alto, a polícia foi chamada e de forma rápida as investigações começaram e assim foram identificados cerca de 22 suspeitos. Dentre eles Andreas Peregudovs suposto líder da operação com ele foram presos mais duas pessoas .

### ESPANHA 2018

Em 26 de março de 2018 a agência de investigação anunciou ter prendido o “CABEÇA” do carbanak conhecido como **DENIS K.** juntamente com mais um grupo comparticipante o COBALT na cidade de Alicante na Espanha.

Em uma investigação liderada pela polícia local da Espanha com a colaboração da aplicação da lei em vários países como empresas de segurança cibernética.

Após investigações chegaram à conclusão que essa pessoa tinha colaborado com vários ciberataques. Cooperando desde 2013, durante buscas em suas propriedades foram encontradas caixas cheias de joias, dois carros BMW e 15 mil bitcoin cerca de 150 milhões de dólares. Cerca 1 milhão de dólares nunca foram encontrados.

# **CONCLUSÕES**

O Carbanak é um dos grupos de cibercriminosos mais sofisticados e preocupantes da atualidade. Suas táticas de ataque a instituições financeiras altamente elaboradas provocaram grandes perdas para bancos e organizações em todo o mundo. A sua capacidade de infiltração, persistência e adaptação às defesas de segurança constitui um desafio constante para o setor financeiro e as autoridades que supervisionam a aplicação da lei. A conclusão é que, apesar de esforços para inibir o Carbanak, a evolução de suas técnicas requer uma vigilância constante e uma colaboração global para amenizar essa ameaça persistente.

# **REFERÊNCIAS BIBLIOGRÁFICAS**

<https://www.enigmasoftware.com/pt/carbanak-remocao/>

<https://www.hardware.com.br/comunidade/codigo-completo/1503953/>

<https://sensorstechforum.com/pt/carbanak-source-code-uploaded-virustotal/>

<https://www.kaspersky.com.br/blog/carbanak-source-code-leaked/11764/>

[https://oglobo.globo.com/economia/espanha-prende-hackers-que-roubaram-mais- de-1-bi-de-bancos-22528529](https://oglobo.globo.com/economia/espanha-prende-hackers-que-roubaram-mais-%20de-1-bi-de-bancos-22528529)