TLP: CLEAR

BOLETIM DE SEGURANÇA

Malware BC vinculado ao QakBot tem novo avanço com acesso remoto e coleta de dados

heimdall
security research

Acesse a nossa nova comunidade através do WhatsApp!

Heimdall Security Research

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

Boletins de Segurança – Heimdall

heimdall
security research
A DIVISION OF ISH

SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

1 INTRODUÇÃO EXECUTIVA

Este relatório de segurança, desenvolvido pela equipe de **Inteligência de Ameaças da ISH, Heimdall**, tem como objetivo proporcionar uma compreensão aprofundada e um dimensionamento preciso das ameaças cibernéticas identificadas. O documento está estruturado em três níveis de abordagem: ***Estratégico***, ***Tático*** e ***Operacional***, garantindo uma visão completa e integrada das ameaças e ações recomendadas.

2 ESTRATÉGICO

2.1 SEGMENTO DE MERCADO

Os alvos potencialmente afetados por essa ameaça que será descrita neste relatório, incluem:

- *Serviços financeiros*
- *Saúde*
- *Varejo*
- *Setor público e governos*
- *Tecnologia*

2.2 IMPACTO FINANCEIRO POTENCIAL

- *Roubo de credenciais e dados financeiros*
- *Perda de propriedade intelectual e dados sensíveis*
- *Custos de resposta e remediação*
- *Multas regulatórias por vazamentos de dados*
- *Prejuízos à reputação*
- *Interrupção operacional*

2.3 OBJETIVO DA AMEAÇA

O objetivo do malware BC/QakBot é obter controle remoto sobre dispositivos infectados, roubar informações confidenciais como credenciais bancárias e dados corporativos, e instalar malwares adicionais para ampliar o impacto. Ele busca manter persistência nos sistemas comprometidos, maximizando os danos financeiros e operacionais às vítimas.

3 TÁTICO

3.1 INFORMAÇÕES SOBRE A AMEAÇA

O QakBot (também conhecido como Qbot), é um malware ativo desde 2007, continua a evoluir e representa uma das ameaças cibernéticas mais perigosas da atualidade. A mais recente variante, apelidada de "**Back.Connect**" (BC), introduz recursos avançados de acesso remoto por conexões reversas, combinados com técnicas aprimoradas de coleta de dados. Essa nova versão reforça o impacto potencial do malware, principalmente em setores críticos, ao permitir maior controle e discrição para os operadores maliciosos. O "Back.Connect" (BC) opera com base em comunicações reversas que dificultam a detecção por sistemas de segurança tradicionais. Essa variante foi desenvolvida para obter maior eficiência na coleta de informações e controle remoto, utilizando engenharia social em campanhas de phishing e vulnerabilidades não corrigidas para se propagar.

3.2 OPERAÇÃO E CAPACIDADE DA AMEAÇA

O BC/QakBot inclui acesso remoto avançado por conexões reversas, coleta extensiva de dados confidenciais e evasão de detecção por soluções de segurança. Sua modularidade permite rápida adaptação a novas defesas e expansão de funcionalidades. É altamente eficiente em comprometer sistemas corporativos e financeiros.

Acesso remoto avançado:

- Utiliza conexões reversas para garantir controle total sobre dispositivos infectados, permitindo operações discretas e persistentes.

Coleta de dados confidenciais:

- Rouba credenciais bancárias, informações financeiras, e dados armazenados em navegadores e sistemas corporativos.

Evasão de detecção:

- Desativa soluções de segurança, utiliza comunicação encriptada e técnicas furtivas para dificultar a identificação.

Propagação lateral:

- Move-se dentro da rede para comprometer outros dispositivos, ampliando o impacto do ataque.

Em uma análise foi possível observar que três dos arquivos possuem datas mais recentes em comparação aos demais, sendo que dois deles compartilham a mesma data, enquanto um arquivo .dat apresenta uma data posterior. Caso o arquivo DLL identificado anteriormente, denominado 'winhttp.dll', presente neste

ZIP, seja carregado pelo OneDriveStandaloneUpdater.exe, há a possibilidade de que o arquivo .dat seja utilizado posteriormente. Além disso, o caminho PDB da DLL sugere que ela pode ter sido projetada para ser carregada de forma lateral.

F:\dbs\sh\odct\1021_111212\client\onedrive\Product\StandaloneUpdater\exe\obj\amd64\OneDriveStandaloneUpdater.pdb

Tabela 1 – OneDriveStandaloneUpdater.exe.

A DLL é responsável por carregar e descriptografar o arquivo .dat mencionado anteriormente, antes de executar a implantação de uma mensagem de teste.

```
mov     [rbp+110h+var_10C], 0
mov     [rbp+110h+var_E8], 0
lea     rcx, aCalculator ; "calculator"
call    sub_180070F72
lea     rdx, [rbp+110h+var_10C]
lea     rcx, aSettingsbackup ; "settingsbackup.dat"
call    j_Decode_and_load_180075A70
xor     r9d, r9d        ; uType
lea     r8, Caption     ; "hi!"
lea     rdx, Text       ; "Hi, I am ok!"
xor     ecx, ecx        ; hWnd
call    cs:MessageBoxA
mov     cs:dword_18018F34C, 1
```

Figura 1 – DLL descriptografando arquivo .dat.

A inicialização do thread do cliente do módulo BC consiste em conectar as funções de baixo nível **createprocess** e **exitprocess** antes de executar sua funcionalidade principal. Na função principal, o módulo verifica se existem cópias de si mesmo em execução e, posteriormente, entra em um loop de suspensão para monitorar uma chave de registro codificada chamada 'Software\TitanPlus'.

3.3 TABELA MITRE ATT&CK

Este tópico apresenta as Táticas, Técnicas e Procedimentos (TTPs) identificados nesta ameaça, conforme o framework MITRE ATT&CK, oferecendo uma visão tática detalhada sobre o comportamento do adversário. O objetivo é permitir o mapeamento das técnicas utilizadas pelos atacantes, facilitando a implementação de contramedidas eficazes e o aprimoramento das defesas de segurança.

Tática	Técnica	Detalhes
Initial Access	T1566.001Phishing: Spearphishing Attachment	Adversários podem enviar e-mails de spearphishing com anexos maliciosos para obter acesso inicial aos sistemas das vítimas.
Execution	T1053.005: Scheduled Task/Job: Scheduled Task	Adversários podem abusar do Agendador de Tarefas do Windows para executar código malicioso de forma inicial ou recorrente.

Privilege Escalation	T1055: Process Injection	Adversários podem injetar código em processos legítimos para escalar privilégios dentro de um sistema.
Defense Evasion	T1218.011: System Binary Proxy Execution: Rundll32	Adversários podem utilizar o rundll32.exe para executar código malicioso, evitando a detecção por soluções de segurança.
Credential Access	T1003: OS Credential Dumping	Adversários podem tentar despejar credenciais para obter materiais de login e credenciais, normalmente na forma de um hash ou senha em texto claro.
Discovery	T1016: System Network Configuration Discovery	Adversários podem procurar detalhes sobre a configuração e as configurações da rede, como endereços IP e/ou MAC, dos sistemas que acessam ou por meio da descoberta de informações de sistemas remotos.
Collection	T1005: Data from Local System	Adversários podem procurar fontes do sistema local, como sistemas de arquivos e arquivos de configuração ou bancos de dados locais, para encontrar arquivos de interesse e dados confidenciais antes da exfiltração.
Command and Control	T1071.001: Application Layer Protocol: Web Protocols	Adversários podem utilizar protocolos da camada de aplicação, como HTTP ou HTTPS, para se comunicar com a infraestrutura de comando e controle.
Exfiltration	T1041: Exfiltration Over C2 Channel	Adversários podem exfiltrar dados através do mesmo canal de comando e controle utilizado para comunicação.

Tabela 2 – Tabela MITRE ATT&CK.

4 RECOMENDAÇÕES

Além dos indicadores de comprometimento elencados abaixo pela ISH, poderão ser adotadas medidas visando a mitigação da infecção da referida *ameaça*, como por exemplo:

Educação e treinamento de usuários

- Realizar treinamentos regulares sobre conscientização em segurança para que os colaboradores reconheçam e evitem e-mails de phishing, anexos maliciosos e links suspeitos.

Atualização de software e aplicação de patches

- Manter sistemas operacionais, navegadores e software atualizados com os últimos patches de segurança, eliminando vulnerabilidades conhecidas exploradas por malwares.

Implementação de autenticação multifator (MFA)

- Adotar MFA para proteger contas críticas, dificultando o acesso de adversários mesmo que credenciais sejam comprometidas.

Monitoramento contínuo e resposta a incidentes

- Configurar soluções de monitoramento de rede e endpoints para detectar atividades anômalas, como comunicação com servidores de comando e controle (C2), e responder rapidamente a incidentes.

Políticas de controle de execução de scripts

- Restringir a execução de scripts desconhecidos, como PowerShell ou executáveis não assinados, e configurar o sistema para exigir permissões administrativas para modificações críticas.

Backups seguros e regularmente testados

- Realizar backups regulares de dados críticos e armazená-los em locais seguros, separados da rede principal, para garantir recuperação em caso de comprometimento.

Segmentação de rede e privilégios mínimos

- Implementar segmentação de rede para limitar o movimento lateral do malware e adotar o princípio do menor privilégio, garantindo que os usuários e sistemas tenham acesso apenas ao necessário.

5 OPERACIONAL

A ISH Tecnologia realiza o tratamento de diversos indicadores de compromissos coletados por meio de fontes abertas, fechadas e também de análises realizadas pela equipe de segurança Heimdall. Diante disto, abaixo listamos todos os Indicadores de Comprometimento (IOCs) relacionadas a análise do(s) artefato(s) deste relatório.

5.1 INDICADORES DE COMPROMETIMENTO (IOC)

Indicadores do artefato	
md5:	a4e3345491eaca250f1cc139db05a015
sha1:	f09804b59a3aac7c1dd47c7e027182fb54f9a277
sha256:	22c5858ff8c7815c34b4386c3b4c83f2b8bb23502d153f5d8fb9f55bd784e764
File name:	PixelSignal.dll

Indicadores do artefato	
md5:	b15afa16da42bc65167060caed1835a4
sha1:	7eb964f0f14c915d0112a2211c4c1ac8eeccba99
sha256:	98d38282563c1fd09444724eacf5283626aeef36bcb3efa9d7a667db7314d81f
File name:	pack.dat

Indicadores do artefato	
md5:	0f0a4795ad4dbd7d5c54d32ae35f308d
sha1:	41bd3fb0740e91267391becb2fbc1f3789dabbf9
sha256:	651e49a45b573bb39e21746cb99fcd5d17679e87e04201f4cc6ca10ff2d166e4
File name:	winhttp.dll

Tabela 3 – Indicadores de Comprometimento

5.2 INDICADORES DE URL, IPS E DOMÍNIOS

Indicadores de URL, IPs e Domínios	
IP	80[.]66[.]89[.]100 146[.]19[.]128[.]138

Tabela 4 – Indicadores de Comprometimento de Rede.

Obs: Os *links* e endereços IP elencados acima podem estar ativos; cuidado ao realizar a manipulação dos referidos IoCs, evite realizar o clique e se tornar vítima do conteúdo malicioso hospedado no IoC.

6 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Medium**
- **Thehackernews**

7 AUTORES

- **Leonardo Oliveira**

heimdall
security research
A DIVISION OF ISH