BOLETIM DE SEGURANÇA

APT-C-60 explorando falha no WPS Office para implantar Backdoor SpyGlace

heimdall
security research
A DIVISION OF ISH

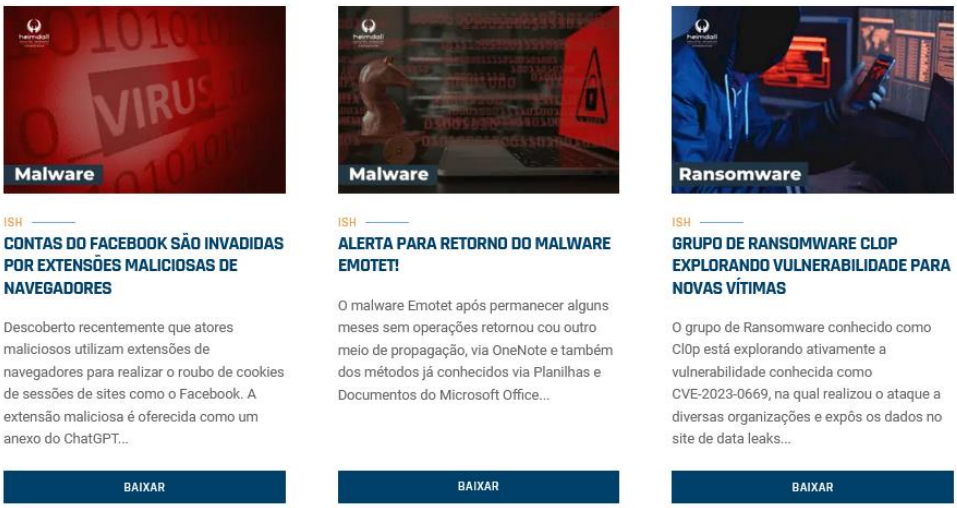
TLP: CLEAR

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso **X**.

[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]



SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

1 SUMÁRIO EXECUTIVO

Pesquisadores identificaram uma vulnerabilidade CVE-2024-7262 de execução de código no WPS Office para Windows categorizada como crítica , explorada pelo grupo de ciberespionagem **APT-C-60**, alinhado à Coreia do Sul. Após análise, foi descoberta uma segunda forma de exploração do código defeituoso (CVE-2924-7263). Ambas as vulnerabilidades foram corrigidas após um processo de divulgação coordenado.

2 INFORMAÇÃO SOBRE A VULNERABILIDADE

Durante uma investigação das atividades do APT-C-60, foi encontrado um documento de planilha que referenciava um componente do downloader do grupo. A análise revelou uma vulnerabilidade de execução de código no WPS Office para Windows, explorada pelo APT-C-60 para atingir países do Leste Asiático. O payload final é um backdoor personalizado chamado SpyGlace, documentado como TaskControler.dll pelo ThreatBook.

Com mais de 500 milhões de usuários ativos globalmente, o WPS Office é um alvo significativo, especialmente na região do Leste Asiático. Durante a divulgação coordenada de vulnerabilidades, a DBAPPSecurity publicou uma análise independente confirmando que o APT-C-60 usou a vulnerabilidade para entregar malware a usuários na China. O documento malicioso (SHA-1: *7509B4C506C01627C1A4C396161D07277F044AC6*) é uma exportação MHTML de uma planilha XLS, contendo um hiperlink oculto projetado para executar uma biblioteca arbitrária ao ser clicado no WPS Spreadsheet. O formato MHTML permite o download de arquivos ao abrir o documento, facilitando a execução remota de código. A figura abaixo mostra o documento no WPS Spreadsheet, com uma imagem de linhas e colunas referenciando a solução de e-mail Coremail, usada como isca para ocultar o hiperlink malicioso.

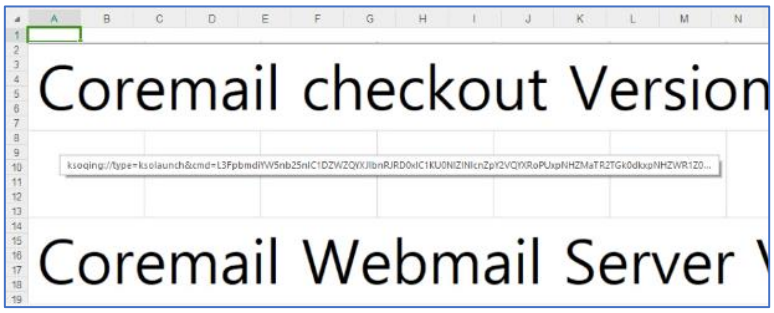


Figura 1 – O documento de exploração incorpora uma imagem ocultando o hiperlink malicioso.

O bug explorado pelo APT-C-60, permite a execução de código ao sequestrar o fluxo de controle do componente do plugin WPS Office, promecefpluginhost.exe. Ao instalar o WPS Office para Windows, o software registra um manipulador de protocolo personalizado chamado ksoqing. Isso permite a execução de um aplicativo externo sempre que um usuário clica em uma URL que começa com o esquema de URI ksoqing://. No Windows, o registro de um manipulador de protocolo personalizado é feito no registro do sistema.

Neste caso, o valor padrão sob a chave HKCR\ksoqing\shell\open\command instrui o Windows a executar C:\Users<USER>\AppData\Local\Kingsoft\WPS Office<VERSION>\office6\wps.exe com o argumento /qingbangong “%1”, onde %1 é substituído pela URL completa. Para ilustrar isso, a Figura 2 mostra o que acontece quando um usuário clica em

um hiperlink usando o protocolo personalizado ksoqing dentro do aplicativo WPS Spreadsheet (et.exe).

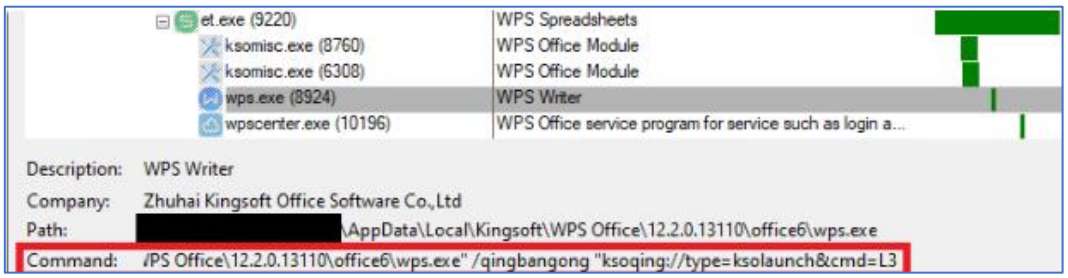


Figura 2 – Aplicativo WPS Spreadsheet iniciando o wps.exe.

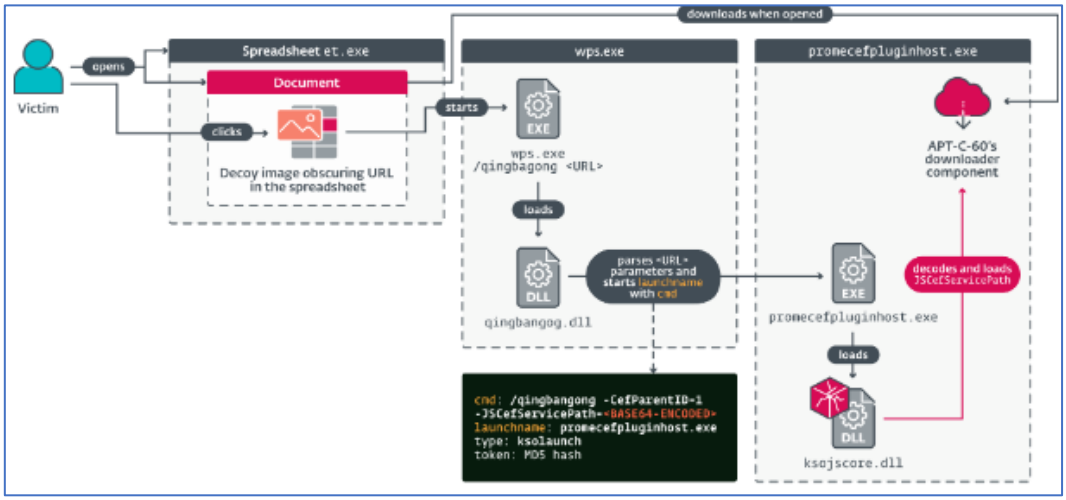


Figura 3 – Visão geral do fluxo de controle do exploit.

Quando o wps.exe é iniciado, ele carrega o qingbangong.dll, responsável por analisar e validar certos parâmetros do hiperlink. O link malicioso encontrado no arquivo de exploração segue o formato ksoqing://type=ksolaunch&cmd=<string codificada em base64>&token=<hash MD5>&launchname=promecefpluginhost.exe. Nossa análise mostrou que isso resulta no lançamento de um aplicativo já presente no sistema (neste caso, promecefpluginhost.exe), com a linha de comando codificada em base64 fornecida pelo invasor.

O parâmetro token é o hash MD5 do valor codificado do parâmetro cmd concatenado com a string *qingLaunchKey* e o valor codificado do parâmetro launchname. Este último deve ser um executável localizado em C:\Users<USER>\AppData\Local\Kingsoft\WPS Office<VERSION>\office6\ e assinado com um certificado válido da Kingsoft.

Ao decodificar o parâmetro cmd, descobrimos que a linha de comando /qingbangong -CefParentID=1 -JSCefServicePath=<caminho do arquivo codificado em base64> é passada para o promecefpluginhost.exe. Após a inicialização, a biblioteca ksojscore.dll é carregada e decodifica o parâmetro JSCefServicePath. O resultado é uma string passada como parâmetro para o método QLibrary::load do Qt. Esse caminho de arquivo é definido pelo invasor, permitindo a execução de código ao carregar uma DLL arbitrária. A Figura 4 ilustra como o parâmetro JSCefServicePath controlado pelo invasor é processado pela ksojscore.dll.

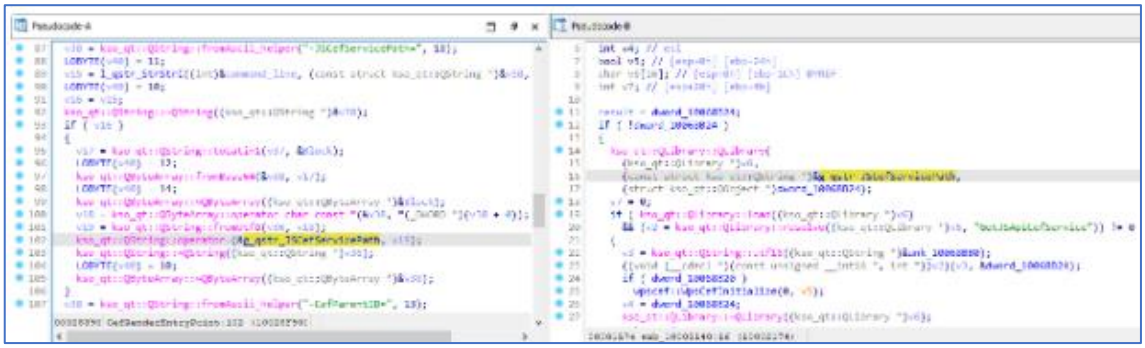


Figura 4 – O parâmetro JSCefServicePath é decodificado (esquerda) e usado como um argumento para o método QLibrary::load (direita).

É possível explorar o protocolo do esquema ksoqing para criar um hiperlink que, ao ser clicado, carregue uma biblioteca de um caminho de arquivo remoto específico. O grupo APT-C-60 utilizou essa vulnerabilidade para executar seu componente de download de trojan de primeiro estágio (SHA-1: *08906644B0EF1EE6478C45A6E0DD28533A9EFC29*). Para explorar essa falha, um invasor precisa armazenar uma biblioteca maliciosa em um local acessível pelo computador alvo, seja no sistema ou em um compartilhamento remoto, e conhecer o caminho do arquivo previamente. Os desenvolvedores do exploit dessa vulnerabilidade conheciam alguns truques para alcançar esse objetivo.

Os criadores do exploit decidiram usar um recurso específico do formato de arquivo MHTML para garantir que seu componente malicioso fosse baixado e armazenado no sistema de forma previsível. Esse formato de arquivo é uma opção de exportação oferecida pelos aplicativos Microsoft Word e Excel, permitindo que os usuários visualizem documentos em seus navegadores. Trata-se de um arquivo multiparte que contém HTML, CSS e JavaScript, facilitando a exibição do documento. Ao inserir uma tag img em um dos arquivos HTML, é possível fazer com que o aplicativo Spreadsheet baixe um arquivo remoto quando o documento é carregado. Por exemplo, a Figura 5 mostra um de nossos arquivos de teste com a tag img e seu elemento src apontando para uma biblioteca armazenada localmente.

```
------=_NextPart_01DAB6E8.8F69D770
Content-Location: file:///C:/E5E78E57/input_files/sheet001.htm
Content-Transfer-Encoding: quoted-printable
Content-Type: text/html; charset="us-ascii"

<html xmlns:v=3D"urn:schemas-microsoft-com:vml"
xmlns:o=3D"urn:schemas-microsoft-com:office:office"
xmlns:x=3D"urn:schemas-microsoft-com:office:excel"
xmlns=3D"http://www.w3.org/TR/REC-html40">

<head>

<img src="http://localhost/Dll1.dll"/>
<meta http-equiv=3DContent-Type content=3D"text/html;
charset=3Dus-ascii">
<meta name=3DProgId content=3DExcel.Sheet>
<meta name=3DGenerator content=3D"Microsoft Excel 15">
<link id=3DMain-File rel=3DMain-File href=3D"../input.htm">
<link rel=3DFile-List href=3Dfilelist.xml>
```

Figura 5 – Inserção da tag img.

Para resolver o problema do caminho de arquivo previsível, foi identificado que os arquivos baixados são armazenados em %localappdata%\Temp\wps\INetCache\, com o nome sendo o hash MD5 da URL codificada em UTF-16LE. Por exemplo, a URL http://localhost/Dll1.dll gera o hash MD5 *914CBE6372D5B7C93ADDC4FEB5E964CD*. No entanto, ao definir a variável JSCefServicePath para esse caminho, ela é concatenada ao diretório raiz do WPS Office em %localappdata%\Kingsoft\WPS Office\<VERSION>\office6\. Se o arquivo não for encontrado, o promecefpluginhost.exe tentará recuperá-lo de outros caminhos.

Um último desafio é que a extensão .dll é anexada ao nome do arquivo quando o promecefpluginhost.exe tenta carregar a biblioteca. A extensão não é anexada ao criar o arquivo baixado. Os autores do exploit usaram a API do Windows para contornar essa restrição. O método QLibrary::Load, que chama LoadLibraryW, permite que adicionar um ponto final (.) ao lpLibFileName impeça a função de anexar .dll. Assim, anexar esse caractere ao caminho relativo permite carregar a biblioteca.

Ao investigar as versões afetadas pela vulnerabilidade inicial, verificações adicionais foram implementadas nos componentes promecefpluginhost.exe e ksojscore.dll para verificar a variável JSCefServicePath. No entanto, a variável CefPluginPathU8 não foi coberta pelo patch. A primeira verificação ocorre quando o promecefpluginhost.exe itera sobre seus argumentos de linha de comando. Se um parâmetro tiver o mesmo nome (sensível a maiúsculas e minúsculas) que uma das variáveis mencionadas, ele é descartado.

```
do
{
  kso_qt::QString::fromWCharArray(&current_argv, argv[i], -1);
  qstr_JSCefServicePath = kso_qt__QString__fromAscii_helper("-JSCefServicePath=", 18);
  v13 |= 1u;
  *discard_arg_flag = v13;
  if ( kso_qt::QString::startsWith(&current_argv, &qstr_JSCefServicePath, 1)
    || (qstr_CefPluginPathU8 = kso_qt__QString__fromAscii_helper("-CefPluginPathU8=", 17),
        v13 |= 2u,
        *discard_arg_flag = v13,
        v15 = kso_qt::QString::startsWith(&current_argv, &qstr_CefPluginPathU8, 1),
        discard_arg_flag[3] = 0,
        v15) )
  {
    discard_arg_flag[3] = 1;
```

Figura 6 – Verificação de código e descarte de parâmetros passados.

Após isso, o caminho de arquivo esperado para JSCefServicePath, onde jscefservice.dll deve ser armazenado, é recuperado. O caminho correto deve ser %LOCALAPPDATA%\Kingsoft\WPS Office<VERSION>\office6\addons\kcef. O mesmo procedimento é aplicado para CefPluginPathU8, cujo caminho deve ser %LOCALAPPDATA%\Kingsoft\WPS Office<VERSION>\office6\addons\cef.

Uma nova linha de comando é criada com os parâmetros aceitos, seguidos pelos caminhos de arquivo identificados pelas variáveis nomeadas. O promecefpluginhost.exe então carrega a biblioteca ksojscore.dll e chama sua exportação CefRenderEntryPoint com a linha de comando reconstruída. Ambas as variáveis são verificadas, mas desta vez a comparação não diferencia maiúsculas de minúsculas.

Aqui surge a primeira falha lógica. Se uma letra das variáveis nomeadas for alterada para maiúscula ou minúscula, a primeira verificação (sensível a maiúsculas e minúsculas) não rejeitará o parâmetro do invasor, e a linha de comando ficará assim:

- *-JSC E fServicePath=<CONTROLADO_PELO_INVASOR> <OUTROS_PARÂMETROS>*
- *-JSCefServicePath=<CAMINHO_REAL>*

Quando essa linha de comando é passada para ksojscore.dll, ela aceitará apenas a primeira ocorrência da variável, e a variável controlada pelo invasor será sempre priorizada. No entanto, antes de carregar a biblioteca indicada pelo caminho JSCefServicePath, uma segunda verificação é feita. A função krt::ksafe::KProcess::verifyZhuHaiKingsoftCertSigner verifica o certificado da biblioteca para garantir que pertence à Kingsoft. Portanto, um invasor não pode carregar qualquer biblioteca arbitrária.

A principal limitação dessa vulnerabilidade é a string libcef.dll anexada ao caminho do arquivo. Até o momento, não encontramos uma maneira de baixar um arquivo e escolher seu nome. No entanto, em uma rede local, hospedar uma biblioteca em um compartilhamento e apontar a variável CefPluginPathU8 para ela funciona, pois LoadLibraryExW permite especificar caminhos de rede.

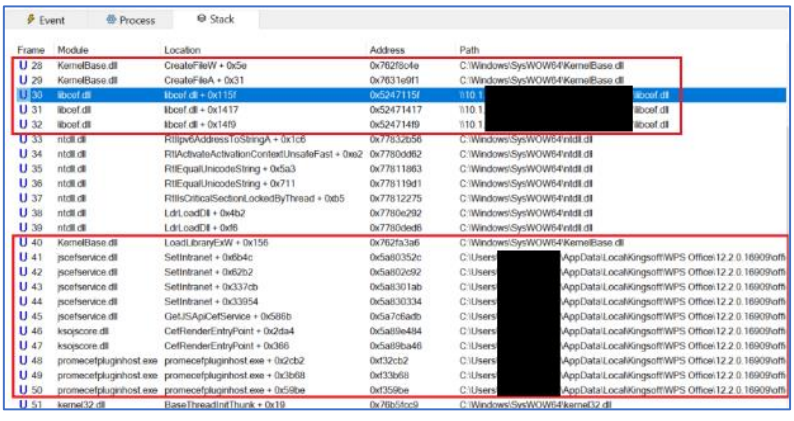


Figura 7 – Visualização da pilha do Procmon.

3 MITRE ATT&CK - TTPs

Tática	Técnica	Detalhes
Resource Development	T1583.001 T1583.004 T1608.001 T1587.004	Consiste em técnicas que envolvem adversários criando, comprando ou comprometendo/roubando recursos que podem ser usados para dar suporte à segmentação.
Execution	T1203 T1204.001	Consiste em técnicas que resultam em código controlado pelo adversário em execução em um sistema local ou remoto.

Tabela 1 – Tabela MITRE ATT&CK.

4 RECOMENDAÇÕES

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

Atualize o WPS Office

- Certifique-se de que o software esteja atualizado para a versão mais recente.

Restrições

- Limite o uso do WPS Office, especialmente das versões 12.2.0.13110 a 12.2.0.13489, em sistemas Windows.

Controle de acesso rigoroso

- Implemente controles de acesso estritos e o princípio do menor privilégio para minimizar o impacto potencial.

Educação dos usuários

- Instrua os usuários sobre os riscos de abrir documentos não confiáveis ou clicar em links suspeitos dentro de documentos.

Monitoramento de rede

- Utilize ferramentas de monitoramento de rede para detectar atividades suspeitas relacionadas ao WPS Office.

Backup regular

- Realize backups regulares dos dados para garantir a recuperação em caso de ataque.

Análise de vulnerabilidades

- Realize análises de vulnerabilidades regularmente para identificar e corrigir possíveis falhas de segurança.

5 INDICADORES DE COMPROMISSOS

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 Compromissos (IOCs) relacionadas a análise do(s) artefato(s) deste relatório.

Indicadores de compromisso do artefato	
md5:	9f88234068d7abad65979eb1df63efb5
sha1:	7509b4c506c01627c1a4c396161d07277f044ac6
sha256:	6174276f94219bc386bdc628ca18eaec261998b7bd03077562fe93c268b42446
File name:	[Coremail]Vuln_Versionlist.et

Indicadores de compromisso do artefato	
md5:	b14ef85a60ac71c669cc960bdf580144
sha1:	08906644b0ef1ee6478c45a6e0dd28533a9efc29
sha256:	861911e953e6fd0a015b3a91a7528a388a535c83f4b9a5cf7366b8209d2f00c3
File name:	Dll1.dll

Tabela 2 – Indicadores de Compromissos de artefatos

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
Domínio	rammenale[.]com
IP	162.222.214[.]48 131.153.206[.]231

Tabela 3 – Indicadores de Compromissos 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**
- Welivesecurity
- Thehackernews
- NVD

7 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH