# BOLETIM DE SEGURANÇA

Utilização do software ScreenConnect para persistências, backdoors e comunicação com C2

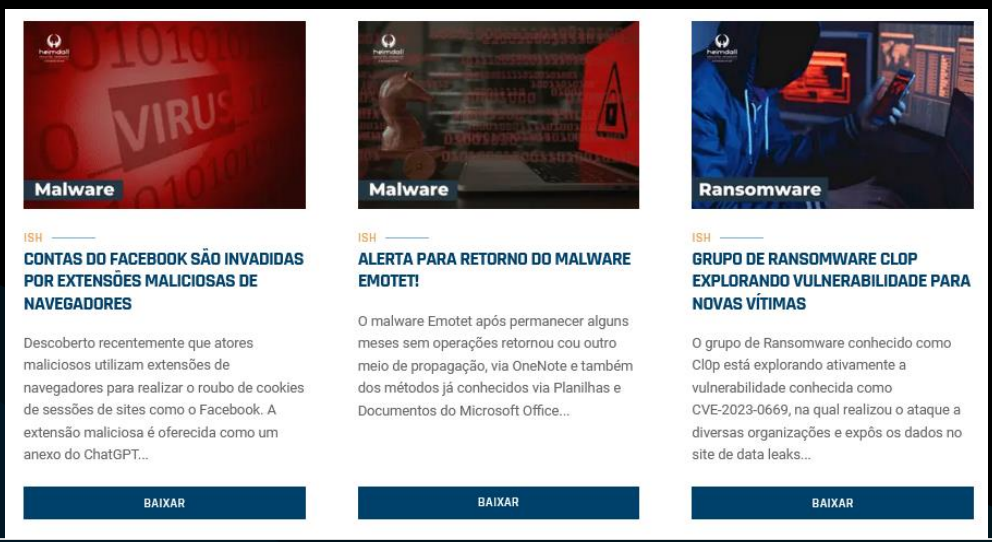
heimdall
security research
A DIVISION OF ISH

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

**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

# Sumário

# Lista de Tabelas

# Lista de Figuras

# 1 SUMÁRIO EXECUTIVO

Atores de ameaças costumam utilizar algumas ferramentas para auxiliar no ataque as organizações, dentre essas ferramentas podemos mencionar a utilização de softwares legítimos, bem como de gerenciamento remoto (RMM).

Desde o início do ano de 2023, a Heimdall observou campanhas utilizando-se de e-mails de phishing que encaminham o usuário a realizar o download de ferramentas de gerenciamento remoto conhecida como **ScreenConnect (ConnectWise Control)**.

A utilização desta ferramenta se dá pelo fato de facilitar a venda de acesso a rede da organização a outros tipos de criminosos cibernéticos como ameaças persistentes avançadas (APT) ou realizar a exfiltração de informações e dados da rede da organização.

Portanto, a ISH menciona os principais recursos apresentados para os atores de ameaças ao utilizarem esta ferramenta e quais os seus riscos para com as organizações.

# 2 Utilização de ferramentas e gerenciamento remoto

Em diversas campanhas maliciosas podemos observar a utilização de softwares de acessos remotos para iniciar os ataques cibernéticos, seja para roubo de informações e dados ou até recursos financeiros (a depender da campanha e motivação dos cibercriminosos).

Os atores de ameaças utilizam estes softwares com o intuito de facilitar a conexão com a infraestrutura já que estes softwares podem ser legítimos e não seriam facilmente detectáveis pelas organizações. A utilização destes softwares normalmente acaba não acionando as defesas de antivírus ou *antimalwares* e, podemos afirmar que os cibercriminosos utilizam esses softwares para garantir *backdoors* para persistência e para C2 (Comando e Controle).

A seguir, abordamos uma destas ferramentas que podem ser utilizadas pelos atores maliciosos, bem como o método de entrega realizada dos artefatos.

# 3 SCREENCONNECT

O software **ScreenConnect** é um software de suporte remoto que permite aos administradores de rede controlar os computadores e dispositivos móveis remotamente e, este é utilizado por empresas de todos os tamanhos para fornecer suporte a clientes, resolver problemas e oferecer treinamento.

A ferramenta foi identificada sendo propagada por meio de uma campanha maliciosa utilizando phishing com um anexo de PDF contendo um link para abrir o arquivo malicioso. Após o usuário clicar no link acaba baixando um executável, um zip e um script dependendo do tipo da campanha utilizada no e-mail.

Assim que o arquivo malicioso baixado for executado, o software ScreenConnect é instalado.

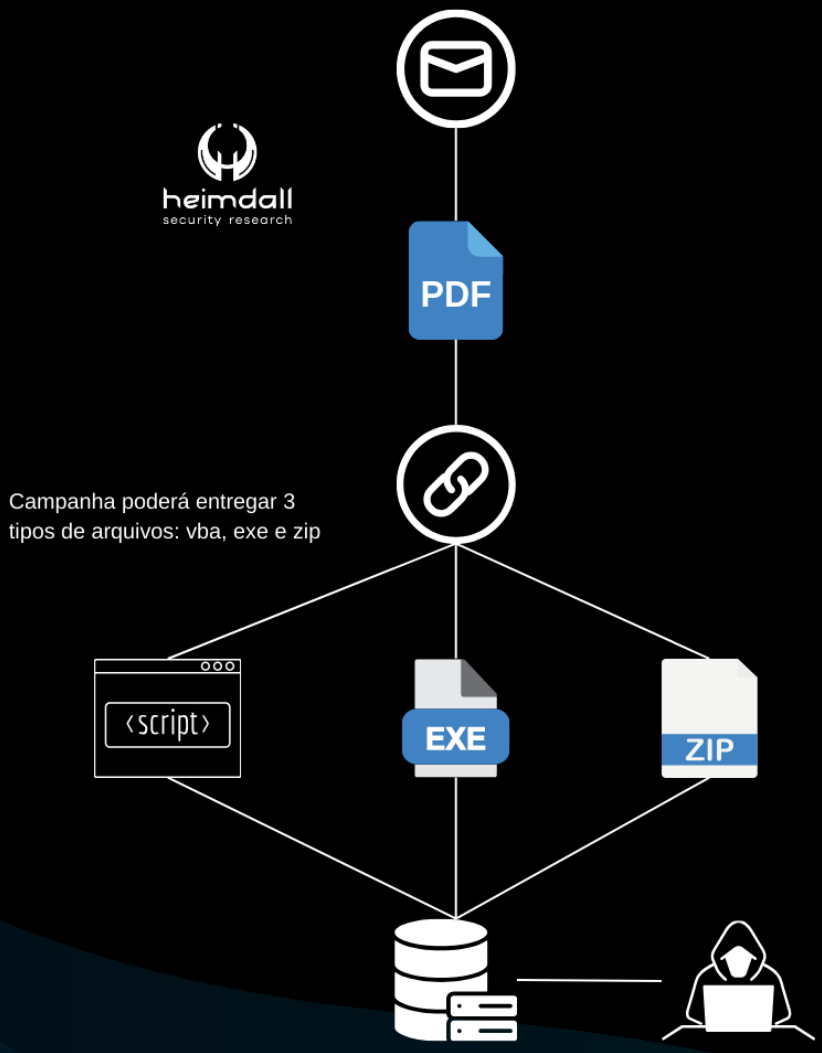
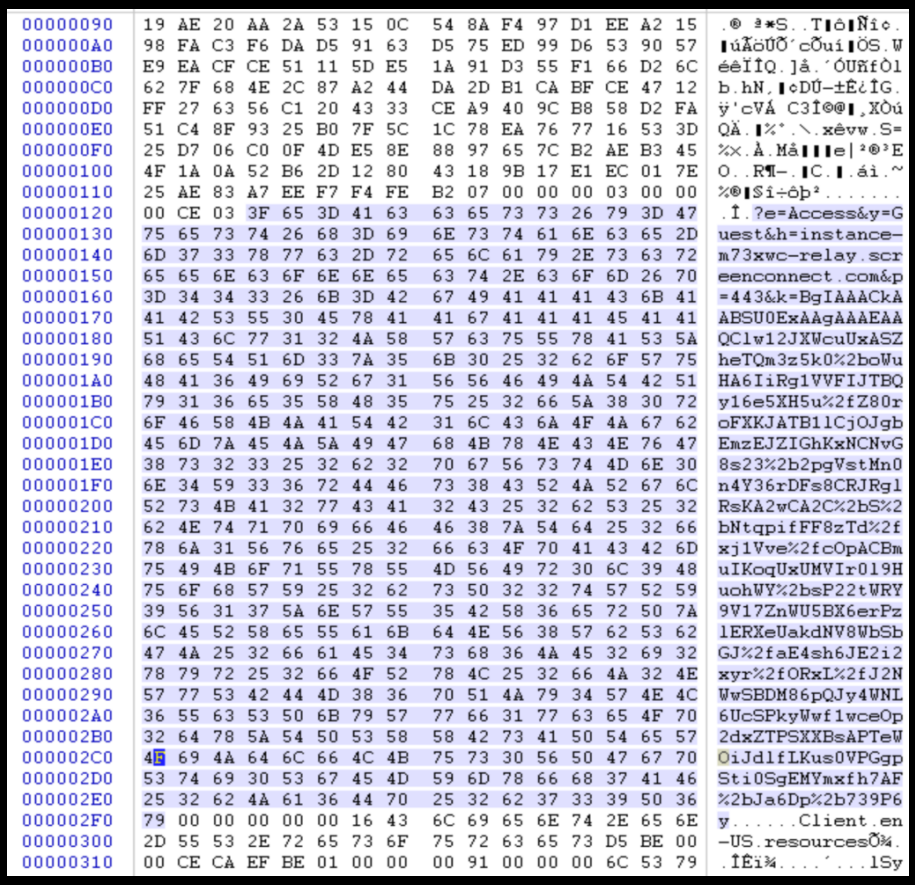



*Figura 1 – Cadeia de infecção de campanhas identificadas distribuindo ScreenConnect.*

A referida campanha utiliza inúmeras URLs de serviços de compartilhamento de arquivos para fins de download de arquivos maliciosos, acrescentando que o software realiza a conexão com a infraestrutura legítima do ConnectWise, dificultando na lista eficaz de indicadores.



| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 00000090 | 19 | AE | 20 | AA | 2A | 53 | 15 | 0C | 54 | 8A | F4 | 97 | D1 | EE | A2 | 15 | .® ª*S..T‹ô—Ñî¢. |
| 000000A0 | 98 | FA | C3 | F6 | DA | D5 | 91 | 63 | D5 | 75 | ED | 99 | D6 | 53 | 90 | 57 | ˜úÃöÚÕ'cÕuí™ÖS.W |
| 000000B0 | E9 | EA | CF | CE | 51 | 11 | 5D | E5 | 1A | 91 | D3 | 55 | F1 | 66 | D2 | 6C | éêÏÎQ.]å.'ÓUñfÒl |
| 000000C0 | 62 | 7F | 68 | 4E | 2C | 87 | A2 | 44 | DA | 2D | B1 | CA | BF | CE | 47 | 12 | b.hN,‡¢DÚ-±Ê¿ÎG. |
| 000000D0 | FF | 27 | 63 | 56 | C1 | 20 | 43 | 33 | CE | A9 | 40 | 9C | B8 | 58 | D2 | FA | ÿ'cVÁ C3Î©@œ¸XÒú |
| 000000E0 | 51 | C4 | 8F | 93 | 25 | B0 | 7F | 5C | 1C | 78 | EA | 76 | 77 | 16 | 53 | 3D | QÄ.“%°.\.xêvw.S= |
| 000000F0 | 25 | D7 | 06 | C0 | 0F | 4D | E5 | 8E | 88 | 97 | 65 | 7C | B2 | AE | B3 | 45 | %×.À.Må‎Ž‎ˆ—e\|²®³E |
| 00000100 | 4F | 1A | 0A | 52 | B6 | 2D | 12 | 80 | 43 | 18 | 9B | 17 | E1 | EC | 01 | 7E | O..R¶-.€C.›.áì.~ |
| 00000110 | 25 | AE | 83 | A7 | EE | F7 | F4 | FE | B2 | 07 | 00 | 00 | 00 | 03 | 00 | 00 | %®ƒ§î÷ôþ².....  |
| 00000120 | 00 | CE | 03 | 3F | 65 | 3D | 41 | 63 | 63 | 65 | 73 | 73 | 26 | 79 | 3D | 47 | .Î.?e=Access&y=G |
| 00000130 | 75 | 65 | 73 | 74 | 26 | 68 | 3D | 69 | 6E | 73 | 74 | 61 | 6E | 63 | 65 | 2D | uest&h=instance- |
| 00000140 | 6D | 37 | 33 | 78 | 77 | 63 | 2D | 72 | 65 | 6C | 61 | 79 | 2E | 73 | 63 | 72 | m73xwc-relay.scr |
| 00000150 | 65 | 65 | 6E | 63 | 6F | 6E | 6E | 65 | 63 | 74 | 2E | 63 | 6F | 6D | 26 | 70 | eenconnect.com&p |
| 00000160 | 3D | 34 | 34 | 33 | 26 | 6B | 3D | 42 | 67 | 49 | 41 | 41 | 41 | 43 | 6B | 41 | =443&k=BgIAAACkA |
| 00000170 | 41 | 42 | 53 | 55 | 30 | 45 | 78 | 41 | 41 | 67 | 41 | 41 | 41 | 45 | 41 | 41 | ABSU0ExAAgAAAEAA |
| 00000180 | 51 | 43 | 6C | 77 | 31 | 32 | 4A | 58 | 57 | 63 | 75 | 55 | 78 | 41 | 53 | 5A | QClw12JXWcuUxASZ |
| 00000190 | 68 | 65 | 54 | 51 | 6D | 33 | 7A | 35 | 6B | 30 | 25 | 32 | 62 | 6F | 57 | 75 | heTQm3z5k0%2boWu |
| 000001A0 | 48 | 41 | 36 | 49 | 69 | 52 | 67 | 31 | 56 | 56 | 46 | 49 | 4A | 54 | 42 | 51 | HA6IiRg1VVFIJTBQ |
| 000001B0 | 79 | 31 | 36 | 65 | 35 | 58 | 48 | 35 | 75 | 25 | 32 | 66 | 5A | 38 | 30 | 72 | y16e5XH5u%2fZ80r |
| 000001C0 | 6F | 46 | 58 | 4B | 4A | 41 | 54 | 42 | 31 | 6C | 43 | 6A | 4F | 4A | 67 | 62 | oFXKJATB1lCjOJgb |
| 000001D0 | 45 | 6D | 7A | 45 | 4A | 5A | 49 | 47 | 68 | 4B | 78 | 4E | 43 | 4E | 76 | 47 | EmzEJZIGhKxNCNvG |
| 000001E0 | 38 | 73 | 32 | 33 | 25 | 32 | 62 | 32 | 70 | 67 | 56 | 73 | 74 | 4D | 6E | 30 | 8s23%2b2pgVstMn0 |
| 000001F0 | 6E | 34 | 59 | 33 | 36 | 72 | 44 | 46 | 73 | 38 | 43 | 52 | 4A | 52 | 67 | 6C | n4Y36rDFs8CRJRgl |
| 00000200 | 52 | 73 | 4B | 41 | 32 | 77 | 43 | 41 | 32 | 43 | 25 | 32 | 62 | 53 | 25 | 32 | RsKA2wCA2C%2bS%2 |
| 00000210 | 62 | 4E | 74 | 71 | 70 | 69 | 66 | 46 | 46 | 38 | 7A | 54 | 64 | 25 | 32 | 66 | bNtqpifFF8zTd%2f |
| 00000220 | 78 | 6A | 31 | 56 | 76 | 65 | 25 | 32 | 66 | 63 | 4F | 70 | 41 | 43 | 42 | 6D | xj1Vve%2fcOpACBm |
| 00000230 | 75 | 49 | 4B | 6F | 71 | 55 | 78 | 55 | 4D | 56 | 49 | 72 | 30 | 6C | 39 | 48 | uIKoqUxUMVIr019H |
| 00000240 | 75 | 6F | 68 | 57 | 59 | 25 | 32 | 62 | 73 | 50 | 32 | 32 | 74 | 57 | 52 | 59 | uohWY%2bsP22tWRY |
| 00000250 | 39 | 56 | 31 | 37 | 5A | 6E | 57 | 55 | 35 | 42 | 58 | 36 | 65 | 72 | 50 | 7A | 9V17ZnWU5BX6erPz |
| 00000260 | 6C | 45 | 52 | 58 | 65 | 55 | 61 | 6B | 64 | 4E | 56 | 38 | 57 | 62 | 53 | 62 | lERXeUakdNV8WbSb |
| 00000270 | 47 | 4A | 25 | 32 | 66 | 61 | 45 | 34 | 73 | 68 | 36 | 4A | 45 | 32 | 69 | 32 | GJ%2faE4sh6JE2i2 |
| 00000280 | 78 | 79 | 72 | 25 | 32 | 66 | 4F | 52 | 78 | 4C | 25 | 32 | 66 | 4A | 32 | 4E | xyr%2fORxL%2fJ2N |
| 00000290 | 57 | 77 | 53 | 42 | 44 | 4D | 38 | 36 | 70 | 51 | 4A | 79 | 34 | 57 | 4E | 4C | WwSBDM86pQJy4WNL |
| 000002A0 | 36 | 55 | 63 | 53 | 50 | 6B | 79 | 57 | 77 | 66 | 31 | 77 | 63 | 65 | 4F | 70 | 6UcSPkyWwf1wceOp |
| 000002B0 | 32 | 64 | 78 | 5A | 54 | 50 | 53 | 58 | 58 | 42 | 73 | 41 | 50 | 54 | 65 | 57 | 2dxZTPSXXBsAPTeW |
| 000002C0 | 4F | 69 | 4A | 64 | 6C | 66 | 4C | 4B | 75 | 73 | 30 | 56 | 50 | 47 | 67 | 70 | OiJdlfLKus0VPGgp |
| 000002D0 | 53 | 74 | 69 | 30 | 53 | 67 | 45 | 4D | 59 | 6D | 78 | 66 | 68 | 37 | 41 | 46 | Sti0SgEMYmxfh7AF |
| 000002E0 | 25 | 32 | 62 | 4A | 61 | 36 | 44 | 70 | 25 | 32 | 62 | 37 | 33 | 39 | 50 | 36 | %2bJa6Dp%2b739P6 |
| 000002F0 | 79 | 00 | 00 | 00 | 00 | 00 | 16 | 43 | 6C | 69 | 65 | 6E | 74 | 2E | 65 | 6E | y.....Client.en |
| 00000300 | 2D | 55 | 53 | 2E | 72 | 65 | 73 | 6F | 75 | 72 | 63 | 65 | 73 | D5 | BE | 00 | -US.resourcesÕ¾. |
| 00000310 | 00 | CE | CA | EF | BE | 01 | 00 | 00 | 00 | 91 | 00 | 00 | 00 | 6C | 53 | 79 | .ÎÊï¾....'...lSy |

*Figura 2 – Configuração da instalação do ScreenConnect com o host de conexão.*

Salientamos que a referida campanha para distribuição do software não é recente, sendo que no ano de 2019 fora identificado os atores de ameaças do **Ransomware Zeppelin** utilizando a ferramenta ScreenConnect para comprometimento de rede, roubo de dados e instalar o Ransomware Zeppelin nos computadores e ativos comprometidos.

De acordo com o relatório publicado na época, os atores utilizaram o software em segundo plano, enquanto aguardava uma conexão de gerenciamento remoto.


*Figura 3 – ScreenConnect instalado na máquina aguardando conexão.*

Além do Zepellin, os operadores do **Ransomware Alphv** foram observados utilizando-se do ScreenConnect como forma de garantia de persistência para prosseguir com o ataque de criptografia. Neste outro caso, os afiliados utilizaram um arquivo **.msi** para realizar a entrega dos artefatos do software de conexão, sendo executado como forma de segundo plano aguardando a conexão do servidor remoto.

Já para ataques que envolvam estados-nações, foram observadas a utilização do software através de uma campanha contra diversos países sendo utilizado por cibercriminosos iranianos, cujo foco principal da campanha seria realizar a espionagem.

Para esta campanha, os atores realizaram o mesmo método de entrega mencionado anteriormente, ou seja, por meio de entrega de e-mails de phishing que direcionam o usuário a realizar o download de artefatos que podem ser utilizados para entregar o próximo estágio ou a instalação do ScreenConnect.

# 4 Conclusão

Os atores de ameaças geralmente possuem como alvo usuários que acabam por utilizar estes softwares de conexões remotas, já que os alvos podem variar de organização para organização, bem como a depender do tipo de campanha maliciosa.

Estes atores podem abusar de uma determinada confiança em utilizar estes softwares, como por exemplo, um usuário recebendo uma comunicação de um suposto help desk afirmando que necessita realizar a instalação de ferramentas de controles remotos para fins de conclusão de uma atualização ou aplicar patches de segurança.

Após a instalação e permissão concedida pelo usuário, o ator de ameaça acaba por ter um acesso através de uma backdoor ou persistência garantida por meio do software, podendo prosseguir com seus estágios de ataques.

Por fim, é de suma importância que as organizações observem a utilização destas ferramentas, bem como campanhas que podem ser direcionadas para a organização com o intuito de realizar a instalação e comprometimento da rede.

# 5 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:

- Desconfie de origens não confiáveis: Evite baixar ou executar programas de fontes que você não conhece, especialmente se eles forem solicitados por meio de e-mails não solicitados ou sites suspeitos.

- Verifique a procedência: Certifique-se sempre da origem do software que pretende baixar. Baixe programas somente de fontes oficiais e confiáveis, garantindo a legitimidade da fonte antes de prosseguir.

- Mantenha seu sistema sempre atualizado: Atualize regularmente seu sistema operacional e todos os programas de software com as últimas correções de segurança para resolver possíveis vulnerabilidades conhecidas.

- Utilize soluções de segurança digital: Faça uso de programas antivírus e *antimalware* confiáveis e atualizados, que podem ajudar a identificar e remover possíveis ameaças.

- Evite abrir links suspeitos: Abster-se de clicar em links ou anexos de e-mails de remetentes desconhecidos ou suspeitos. Certifique-se sempre da autenticidade de um e-mail antes de tomar qualquer medida.

- Reforce suas credenciais e adote autenticação de dois fatores (2FA): Proteja suas contas com senhas robustas e habilite a autenticação de dois fatores sempre que possível, tornando o acesso não autorizado mais difícil.

- Familiarize-se com táticas de phishing: Esteja ciente das estratégias de phishing e saiba reconhecer e-mails ou mensagens suspeitas que possam tentar persuadi-lo a baixar software malicioso.

- Invista em treinamento em segurança cibernética: Eduque-se e forneça treinamento para sua equipe, se aplicável, sobre as melhores

práticas em segurança digital. A conscientização é essencial para prevenir ameaças.

- Use com cautela o acesso remoto: Se você necessita utilizar software de acesso remoto, assegure-se de que ele seja proveniente de uma fonte confiável e utilize-o com cuidado. Proteja suas credenciais e ative recursos de segurança, como autenticação de dois fatores.

- Faça backups regulares de seus dados críticos: Realize cópias de segurança periodicamente de seus dados importantes. Isso pode ajudar a recuperar informações em caso de ataques de malware.

# 6 IoCs

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 de artefato malicioso/ analisado | |
|---|---|
| **md5:** | 2cd569dafe4f537150f0416b021c30ab |
| **sha1:** | 3cf40758a15faf5037a7fcb6c8d6c322ec54dfc1 |
| **sha256:** | 31a35e3b87a7f81449d6f3e195dc0660b5dae4ac5b7cd9a65a449526e8fb7535 |
| ***File name:*** | مشروع .docx |

| Indicadores de compromisso de artefato malicioso/ analisado | |
|---|---|
| **md5:** | e8e84ac1ae83a45c260df146e97cb1cb |
| **sha1:** | c58370b4114d4d493e141a66cd1484573ccf02b5 |
| **sha256:** | 3e4e179a7a6718eedf36608bd7130b62a5a464ac301a211c3c8e37c7e4b0b32b |
| ***File name:*** | لمنح الدراسية .exe |

| Indicadores de compromisso de artefato malicioso/ analisado | |
|---|---|
| **md5:** | a8fce1e8e89053e143b5431cfa5209cb |
| **sha1:** | 707c251833db0fb7c17c79413ddaebcb54cdb0fc |
| **sha256:** | 5bfb635c43eb73f25f4e75961a715b96fa764bbe096086fc1e037a7869c7878b |
| ***File name:*** | httpsmod.gov.kw.exe |

| Indicadores de compromisso de artefato malicioso/ analisado | |
|---|---|
| **md5:** | 960594cbdf938bcb03bd0637843d9154 |
| **sha1:** | f228e772a31b4fc160cb59cf5627224613f10941 |
| **sha256:** | b2f429efdb1801892ec8a2bcdd00a44d6ee31df04721482a1927fc6df554cdcf |
| ***File name:*** | _____ _____ .zip |

| Indicadores de compromisso de artefato malicioso/ analisado | |
|---|---|
| **md5:** | b9cff91be734e2a071d3b0fc07dc8386 |
| **sha1:** | 116646a11967c1eed0e6072150b8d581bcf8d6a5 |
| **sha256:** | 77505dcec5d67cc0f6eb841f50da7e7c41a69419d50dc6ce17fffc48387452e1 |
| ***File name:*** | httpsmod.gov.kw.zip |

| Indicadores de compromisso de artefato malicioso/ analisado | |
|---|---|
| **md5:** | fee6ba9a0d7a805b3281d4f955821c1c |
| **sha1:** | 0daea8972337a35f6d48eb9f9dc11ca178dd5e94 |
| **sha256:** | 3b332273cc839a39aa8d37a6094217e5d6d9bf02ef0e8404cd6b3a4b42489251 |
| ***File name:*** | on.exe |

| Indicadores de compromisso de artefato malicioso/ analisado | |
|---|---|
| **md5:** | a047bfe20c52c21bc6060ff0f763c235 |
| **sha1:** | cd300c6a2c22a95b4e5f990ed32b8f429b532328 |
| **sha256:** | ec67af31e0d4ca7f7b449a52468f8b206f5ac0703f5d745499b4e863c4816607 |
| ***File name:*** | RainDrop.exe |

| Indicadores de compromisso de artefato malicioso/ analisado | |
|---|---|
| **md5:** | 79e6f2e1a2a967cbee8803b244fdff72 |
| **sha1:** | e51d26097505137367abce02a6bd1ef242967615 |
| **sha256:** | a656947bcc659d1465ad91dcf8f2cab6d0ae17918eeb0cbf7408b6a8b062adb1 |
| ***File name:*** | Recivutta.vbs |

| Indicadores de compromisso de artefato malicioso/ analisado | |
|---|---|
| **md5:** | 736f8c7459170ca6818e5ca06c440711 |
| **sha1:** | 330d836bb60d50b9b6d5769f9e15579fbb5d8834 |
| **sha256:** | ddb93981561e8538fc75eaec73506f5498b2b0bd504c79ed079ed223b13a63c4 |
| ***File name:*** | ofertaprezi.pdf |

| Indicadores de compromisso de artefato malicioso/ analisado | |
|---|---|
| **md5:** | 334df8989da06aff9a71ab0f6534301a |
| **sha1:** | 0a51c6c7555be78bba9c0dc24b00ac96a51930ed |
| **sha256:** | af5a12a388a7bf416d11b3123251e422f5fd94501e893d11e4fa91de3cb13220 |
| ***File name:*** | bb.exe |

| Indicadores de compromisso de artefato malicioso/ analisado | |
|---|---|
| **md5:** | 7d67a39fdb01fcf50e3cb0b385d37ba2 |
| **sha1:** | 912d6ac12b7be744aa3b3b805c03857c3e43925f |
| **sha256:** | b84f83141e3b56a610fe0c3dd672fcf8f0846ec973d22e8b56e306aa2739e040 |
| ***File name:*** | Fattura 2202855RS.pdf |

| Indicadores de compromisso de artefato malicioso/ analisado | |
|---|---|
| **md5:** | ff139aa66d20be99c34f5e9daec7726b |
| **sha1:** | 6f3500c343c7ec13e7ab3b304df735a0b96f29a3 |
| **sha256:** | 8af109464910afb8c5dc0e1e3c47c58eb6d44c7cbe1b1c2d0dc2979cf5cb5ea9 |
| ***File name:*** | PaymentProf.zip |

| Indicadores de compromisso de artefato malicioso/ analisado | |
|---|---|
| **md5:** | 302ed52d9459e06cc2d4b81de0e2295c |
| **sha1:** | 73049a2f4f19b01adb05df3c3d073cb6066169e6 |
| **sha256:** | c4c0df629f8dbb15bf56089c1bb1f31e4fcc485376ec771942a997bb1654ee9b |
| ***File name:*** | PaymentProofsigned.exe |

Tabela 1 – Indicadores de Compromissos de artefatos.

## URLs de distribuição e endereços IP C2:

| |
|---|
| 149[.]202[.]216[.]53 |
| https[:]//ws[.]onehub.com/files/94otjyvd |
| https[:]//ws[.]onehub.com/files/7w1372el |
| instance-sy9at2-relay[.]screenconnect[.]com |
| instance-uwct38-relay[.]screenconnect[.]com |
| instance-m73xwc-relay[.]screenconnect[.]com |
| https[:]//www.mediafire[.]com/file_premium/b7axm7b5mo2p3az/Recivutta[.]vbs/file" |
| https[:]//www.dropbox[.]com/scl/fi/q7koxcyug90zcutj2dwsh/simple.ghf?rlkey=1qi40k7ozkrev1govodhdxv8i&dl=1 |
| https[:]//t[.]ly/IddaZ |
| https[:]//247info[.]click/DocRecevutta.exe |

Tabela 2 – Indicadores de Compromissos de Rede, Domínios e C2.

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.

# 7 REFERÊNCIAS


- **Heimdall *by* ISH Tecnologia**
- **ScreenConnect utilizado pelo Ransomware Zeppelin**

heimdall
security research
A DIVISION OF ISH