



# BOLETIM DE SEGURANÇA

Campanha do Malware DarkGate



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](#)



ISH

### CONTAS DO FACEBOOK SÃO INVADIDAS POR EXTENSÕES MALICIOSAS DE NAVEGADORES

Descoberto recentemente que atores maliciosos utilizam extensões de navegadores para realizar o roubo de cookies de sessões de sites como o Facebook. A extensão maliciosa é oferecida como um anexo do ChatGPT...

BAIXAR



ISH

### ALERTA PARA RETORNO DO MALWARE EMOTET!

O malware Emotet após permanecer alguns meses sem operações retornou com outro meio de propagação, via OneNote e também dos métodos já conhecidos via Planilhas e Documentos do Microsoft Office...

BAIXAR



ISH

### GRUPO DE RANSOMWARE CLOP EXPLORANDO VULNERABILIDADE PARA NOVAS VÍTIMAS

O grupo de Ransomware conhecido como Cl0p está explorando ativamente a vulnerabilidade conhecida como CVE-2023-0669, na qual realizou o ataque a diversas organizações e expôs os dados no site de data leaks...

BAIXAR

## Sumário

1	Sumário Executivo .....	6
2	Informações coletadas .....	7
3	Conclusão .....	11
4	Recomendações.....	12
5	IoCs .....	13
6	Referências.....	15

## Lista de Tabelas

Tabela 1 – Indicadores de Compromissos.....	14
Tabela 2 – Indicadores de Compromissos de Campanhas de Rede .....	14

## Lista de Figuras

Figura 1 – Captura de tela realizada pela equipe de pesquisa ZeroFox. ....	6
Figura 2 – Campanha de phishing para distribuir o malware identificado pelo pesquisador 0xToxin. ....	7
Figura 3 – Arquivos .cab relacionados ao arquivo extraído. ....	8
Figura 4 – magic bytes do arquivo de script AutoIT. ....	8
Figura 5 – magic bytes do arquivo de script AutoIT identificado. ....	9
Figura 6 – Despejo do arquivo .exe (MZP) malicioso correspondente ao Loader. ....	9

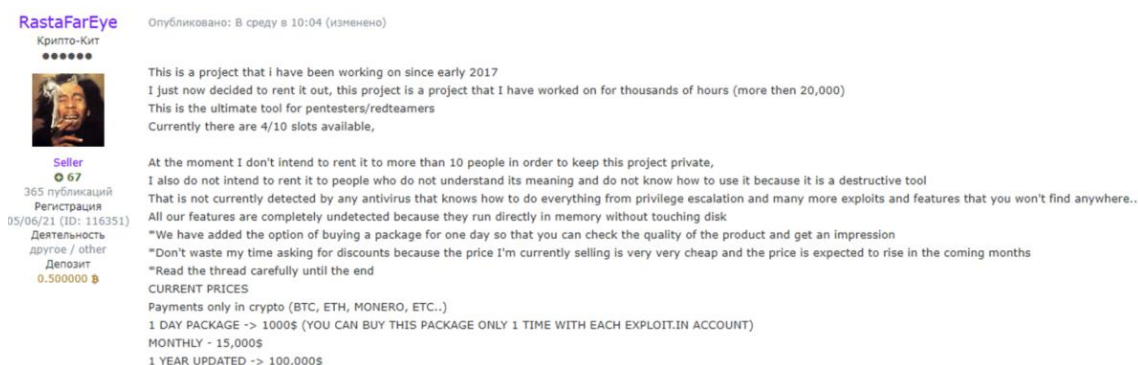
## 1 SUMÁRIO EXECUTIVO

---

A equipe de Inteligência da ISH, coletou informações sobre um malware documentado e identificado pela primeira vez em 2018 conhecido e apelidado como **DarkGate** (também conhecido como MehCrypter).

Este malware é o *loader* de commodities com recursos que incluem a capacidade de baixar e executar arquivos na memória, incluindo um módulo *Hidden Virtual Network Computing (HVNC)*, *keylogging*, roubo de informações e escalonamento de privilégios. O malware utiliza arquivos AutoIT legítimos e normalmente executa vários scripts.


Além disso, foi identificado que novas versões do malware DarkGate estaria sendo anunciado em um fórum Russo desde maio de 2023.



RastaFarEye Опубликовано: В среду в 10:04 (изменено)

Крипто-Кит

\*\*\*\*\*



Seller  
67

365 публикаций  
Регистрация  
05/06/21 (ID: 116351)

Дейтельность  
другое / other  
Депозит  
0.500000 ₪

This is a project that I have been working on since early 2017  
I just now decided to rent it out, this project is a project that I have worked on for thousands of hours (more then 20,000)  
This is the ultimate tool for pentesters/redteamers  
Currently there are 4/10 slots available,

At the moment I don't intend to rent it to more than 10 people in order to keep this project private,  
I also do not intend to rent it to people who do not understand its meaning and do not know how to use it because it is a destructive tool  
That is not currently detected by any antivirus that knows how to do everything from privilege escalation and many more exploits and features that you won't find anywhere..  
All our features are completely undetected because they run directly in memory without touching disk  
\*\*We have added the option of buying a package for one day so that you can check the quality of the product and get an impression  
\*\*Don't waste my time asking for discounts because the price I'm currently selling is very very cheap and the price is expected to rise in the coming months  
\*\*Read the thread carefully until the end

CURRENT PRICES  
Payments only in crypto (BTC, ETH, MONERO, ETC..)  
1 DAY PACKAGE -> 1000\$ (YOU CAN BUY THIS PACKAGE ONLY 1 TIME WITH EACH EXPLOIT.IN ACCOUNT)  
MONTHLY - 15,000\$  
1 YEAR UPDATED -> 100,000\$

Figura 1 – Captura de tela realizada pela equipe de pesquisa ZeroFox.

Portanto, a ISH realizou a coleta de informações e compilou estas neste alerta, visando compartilhar detalhes da operação deste malware contra sistemas informáticos.

## 2 INFORMAÇÕES COLETADAS

---

Em junho, um ator de ameaça com o nome **“RastaFarEye”** teria anunciado um malware multifuncional apelidado de **DarkGate** em um fórum da Deep Web conhecido como “Exploit”. O malware teria sido desenvolvido de forma privada e permitia que os agentes de ameaças construíssem as suas próprias botnets.

O malware possuía **recursos adicionais** como:

- Geração de arquivos .lnk maliciosos
- Tamanho do arquivo pequeno (490kb)
- Execução na memória do sistema
- Ofuscação de payloads para evitar a detecção pelas verificações dinâmicas da maioria dos produtos antivírus.
- Mantém o acesso às máquinas comprometidas durante as reinicializações do sistema.
- Rouba dados confidenciais de navegadores da web.
- Registra as teclas digitadas.
- Obtém permissões de nível superior em máquinas comprometidas
- Utilização dos recursos da máquina comprometida para mineração de criptomoedas.

Além disso, o **preço da licença** do malware pode variar:

- US\$100.000 por ano
- US\$15.000 por mês
- US\$1.000 por dia

Com base em pesquisas, foi possível identificar que o malware DarkGate estaria sendo distribuído com amplas campanhas de phishing, terminando com a implantação do malware como forma de *loader*.

De acordo com relatórios tornados públicos de incidente de segurança, foi possível identificar que o malware DarkGate estaria sendo distribuído por meio de campanhas de phishing.

---

Hello,

Feel free to view & looked over my latest collaboration plan in the url provided below.

<https://becelebrity.com/rj/c1r1vl18p5>

Figura 2 – Campanha de phishing para distribuir o malware identificado pelo pesquisador [OxToxin](#).

Além da campanha, outra campanha observada pela AON foi publicada, na qual pode verificar que ambas as campanhas utilizaram um arquivo .MSI (Microsoft Software Installer) para propagação do malware.

Primeiro, vamos focar na análise publicada pelo pesquisador OxToxin, na qual identificou que era realizado o download do arquivo **“Project\_[0-9]{7}\.msi”**.

O arquivo baixado continha dois arquivos incorporados:

- CustomAction.dll
- WrappedSetupProgram.cab

A DLL é chamada pelo MSI para descompactar o conteúdo armazenado em WrappedSetupProgram.cab e executá-lo.

O arquivo **.cab** inclui dois arquivos:

- Autoit3.exe
- UGtZgHHT.au3 (scripts AutoIT)

..		File folder	
Autoit3.exe	893,608	? Application	7/24/2023 6:10 ...
UGtZgHHT.au3	775,656	? Autolt v3 Script	7/24/2023 6:10 ...

Figura 3 – Arquivos .cab relacionados ao arquivo extraído.

O arquivo script AutoIT identificado começava com os magic bytes:

A3 48 4B BE e 41 55 33 21 45 41 (AU3!EA).

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	A3	48	4B	BE	98	6C	4A	A9	99	4C	53	0A	86	D6	48	7D	£HK~1J@*LS.+0H}
00000010	41	55	33	21	45	41	30	36	4D	A8	FF	73	24	A7	3C	F6	AU3!EA06M`ys\$S<ó
00000020	7A	12	F1	67	AC	C1	93	E7	6B	43	CA	52	A6	AD	00	00	z.ñg-Á`çkCÉR!...
00000030	E1	BB	3A	21	A5	29	E3	EC	E7	0B	98	2E	40	BD	E1	9A	á»:!¥)âiç.`.@%áš
00000040	DE	80	46	B1	9D	6B	3B	21	D4	B1	D6	75	3A	C8	3D	C6	èFf.k;!Ô±Ôu:È=È
00000050	D0	33	F7	14	AF	CB	17	A2	94	01	8D	13	88	FE	64	95	Ð3+.~È.c"...`pd•
00000060	61	E7	B6	4D	1C	F8	00	00	44	9E	CF	F5	FB	39	8D	B6	açM.ø..DžIôú9.ŕ
00000070	75	32	D8	81	2B	0C	DA	5E	B6	04	5E	C5	7A	40	FB	5D	u20.+..Ū^ŕ.^Åz@ú]
00000080	FD	46	87	65	05	A9	4B	51	69	A0	2C	FD	E0	C0	8D	A0	ýF+e.@KQi ,yâÀ.
00000090	F2	1F	6D	0C	C3	8B	25	1A	D6	E1	99	C2	C8	DA	77	34	ò.m.Å<*.Ôá^ÆŪw4
000000A0	23	ED	F9	0C	FA	C7	66	BB	BB	C5	5C	1E	CE	7A	86	9A	#iù.úÇf»»À\..İz+š
000000B0	7D	29	B0	F3	34	10	6D	BD	11	E2	E8	76	73	EF	10	BF	})°ó4.mš.âevsi.¿
000000C0	F0	DA	A4	66	A7	17	62	0B	B8	4F	96	3F	B3	49	38	97	šŪwf\$.b.,O-?°I8-
000000D0	9E	6F	D6	EF	D0	4B	85	2C	D4	96	71	6E	D1	FD	19	44	žoŌiĐK.,Ō-qñŸy.D
000000E0	00	BC	87	00	00	BC	87	00	00	84	A6	00	00	B7	50	D2	.++.+.+.+.+.+.PŌ
000000F0	01	EA	89	DF	02	B7	50	D2	01	EA	89	DF	02	6B	43	CA	.èñš. .PŌ.èñš.kCÈ
00000100	52	AF	AD	00	00	E6	FB	25	78	C8	E2	13	F9	7D	1D	ED	R...èúšxÈ.à.ù).i
00000110	DD	71	00	B0	55	2D	AC	9A	D5	28	15	D4	F0	CF	25	E4	Ÿq.°U--šŌ(.ŌšIèš
00000120	CF	11	8E	56	C2	CE	3F	70	EF	B9	68	60	F8	00	00	35	Ī.ZVĀĪ?pi+h'ø..S
00000130	35	0A	53	5A	5F	53	8C	5E	71	E7	F8	78	CC	0A	01	1B	S.SZ_SE^qçøxĪ...
00000140	09	67	3E	69	30	E2	97	D6	1C	40	1D	B5	BC	37	78	65	.g>i0â-Ō.è.µ47xe

Figura 4 – magic bytes do arquivo de script AutoIT.



No script analisado pelo pesquisador foi observado uma quantia substancial de dados que pareciam ser inúteis, sendo localizado os magic bytes após a quantidade de dados aparentemente inúteis.

```

000A0A00 73 70 50 77 56 63 4F 56 61 56 4C 42 6B 61 49 69 spPwvcOVavLBka11
000A0A10 67 42 43 76 69 7A 51 58 7A 62 58 69 4E 62 41 4C gBCvzQXzbXiNBAL
000A0A20 4B 72 57 53 79 47 74 6B 42 5A 51 74 71 46 53 6D KrWSyGtKbZQtqFSm
000A0A30 63 55 79 4C 44 44 51 6E 46 57 56 59 76 77 44 69 cUyLDDQnFWVYvWdi
000A0A40 78 4E 6C 4E 72 75 69 52 41 4C 4B 70 A3 48 4B BE xNlNruIRALKpLHK%
000A0A50 98 6C 4A A9 99 4C 53 0A 86 D6 48 7D 41 55 33 21 ~lJ@^LS.tOH)AU3!
000A0A60 45 41 30 36 4D A8 FF 73 24 A7 3C F6 7A 12 F1 67 EA06M"y@$$<0z.ñg
000A0A70 AC C1 93 E7 6B 43 CA 52 A6 AD 00 00 E1 BB 3A 21 -Á"çkCÈR!...á»:!
000A0A80 A5 29 E3 EC E7 0B 98 2E 40 BD E1 9A DE 80 46 B1 ¥)ãic".@:ásšPEF±
000A0A90 9D 6B 3B 21 D4 B1 D6 75 3A C8 3D C6 D0 33 F7 14 .k;!ÔiÔu:È=ÈD3÷.
000A0AA0 AF CB 17 A2 94 01 8D 13 88 FE 64 95 61 E7 B6 4D `È.c"...`pd•aqçM
000A0AB0 62 F8 00 00 6C FE 74 84 6A 78 49 F1 B5 91 05 38 bø..lpt„jxIñu`.8
000A0AC0 EE 76 1E F9 D2 72 0B 54 8D 83 9D 74 78 48 10 8D iv.ùÒr.T.f.txH..
000A0AD0 21 E7 DC 29 39 38 4F B5 FD 09 2C EA 58 4F 67 3B !çÜ)98Ouy.,ãXG5;
000A0AE0 4D 6D 98 3D 98 98 41 A4 FC 46 50 57 57 D9 EC 9B Mm"=-"AúFPWWÜi>
000A0AF0 AA DC AC 99 CD 59 15 9D D0 24 63 B5 1A 46 E2 4B *Ü-~mIY..Đçqu.FâK
000A0B00 78 DB 19 FA 69 C4 FE 66 33 1D 48 D3 F6 07 DB 32 xÜ.úíÄpf3.HÖö.Ü2
000A0B10 29 05 E4 C6 3C AC 39 8D 6D 0F 0F F4 80 C1 26 D4 )..ãE<-9.m..öEÁ&ö
000A0B20 F7 FD 34 19 B1 B2 B2 52 0B 0A 90 17 37 0A 3F 87 -ý4.±²²R...7.??#
000A0B30 27 7F 46 15 F5 B9 F7 68 00 BC 87 00 00 BC 87 00 '.F.Á³+h.4±..4±#.

```

Figura 5 – magic bytes do arquivo de script AutoIT identificado.

O script AU3 consistia em dois componentes principais:

1. Um *shellcode* segmentado com codificação hexadecimal que é concatenado em uma única variável.
2. Injeção e execução do *shellcode*.

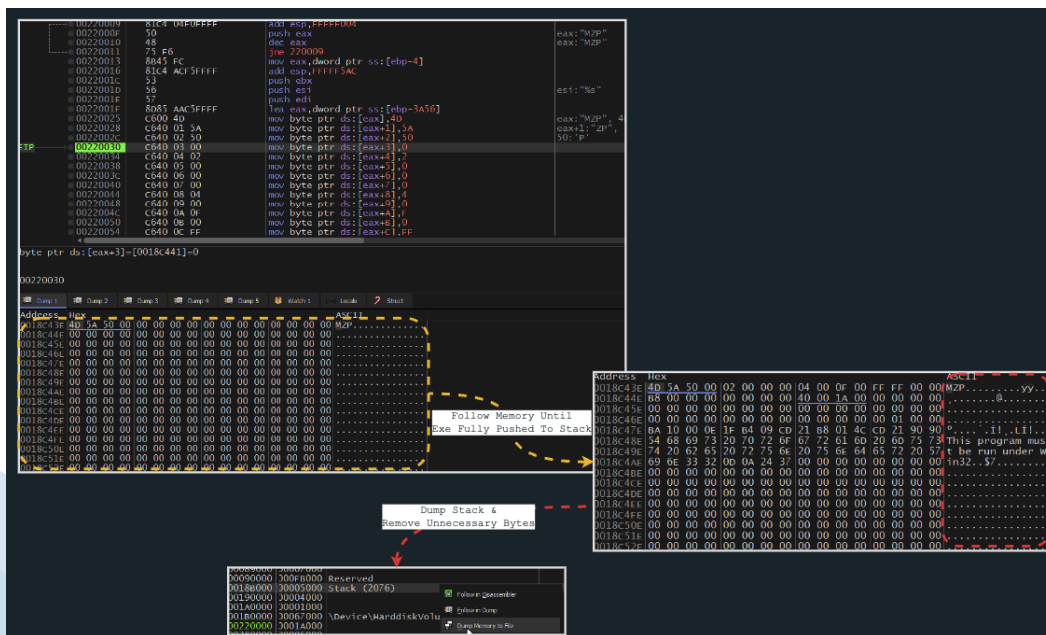


Figura 6 – Despejo do arquivo .exe (MZF) malicioso correspondente ao Loader.

O foco do pesquisador foi em identificar as strings relacionadas ao **Comando e Controle (C2)** utilizados pelos atores de ameaças. Algumas strings decodificadas pelo pesquisador apresentou algumas mensagens de notificações enviadas ao C2, como:

- New Bot: DarkGate is inside hAnyDesk user with admin rights
- DarkGate not found to get executed on the new hAnyDesk Desktop, Did you enabled Startup option on builder?
- Credentials detected, removing them!

Inclusive, a lista contendo todas as strings possíveis identificadas e decodificadas [aqui](#). Incluindo o canal de C2 utilizado na análise do DarkGate: **http[:]//80.66.88[.]145**.

Portanto, é possível observar que o malware utilizada codificação em **base64** para ofuscação das strings, sendo publicado um script [IDAPython](#) para auxiliar na identificação das strings ofuscadas pelo malware.

### 3 CONCLUSÃO

---

Com base nas informações coletadas, a campanha utilizada como forma global utiliza threads de e-mails para phishing, levando o usuário a download do malware sofisticado como o DarkGate.

Os usuários que baixaram o malware receberam um arquivo MSI com dois arquivos incorporados que carregaram o *shellcode* codificado para execução, sendo que o DarkGate também utilizou decodificação exclusiva para duas strings incorporadas, relevando comandos enviados ao C2 e a configuração do malware.

Algumas técnicas de ofuscação como "Loop XOR" e decodificação Base64 personalizada foi observada nas atividades de rede.

## 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:

- Seja desconfiado de todos os e-mails, mensagens de texto e telefonemas. Não clique em links ou abra anexos em e-mails de remetentes desconhecidos.
- Verifique o endereço de e-mail do remetente. Os e-mails de phishing geralmente vêm de endereços de e-mail que parecem legítimos, mas podem ter pequenas diferenças, como uma letra trocada ou um domínio diferente.
- Preste atenção aos erros de ortografia e gramática. Os e-mails de phishing geralmente contêm erros de ortografia e gramática, o que pode ser um sinal de que o e-mail não é legítimo.
- Não se apresse em fornecer informações. Se você receber um e-mail que solicite informações confidenciais, não as forneça até ter certeza de que o e-mail é legítimo.
- Use um antivírus atualizado. Um antivírus atualizado pode ajudar a proteger seu computador contra malware, que às vezes é usado em ataques de phishing.
- Use uma senha forte e única para cada conta. Isso tornará mais difícil para os cibercriminosos invadirem suas contas.
- Atualize seu software regularmente. As atualizações de software geralmente incluem correções de segurança que podem ajudar a proteger seu computador contra ameaças.
- Esteja ciente das últimas tendências em ataques de phishing. Os cibercriminosos estão constantemente desenvolvendo novas técnicas de phishing, por isso é importante estar ciente das últimas tendências para que você possa se proteger.

## 5 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	
<b>md5:</b>	793c0217717b0a37794f7c3adbeda577
<b>sha1:</b>	613a0158629bd9cdcbae1fe411358161645d8a69
<b>sha256:</b>	fadabbf0ef32b7295b5c0dc1830816c35bce50ec9256d01a600d06f346a161d7
<b>File name:</b>	eeabfcb.au3

Indicadores de compromisso de artefato malicioso/ analisado	
<b>md5:</b>	e0d96c0fdcd06ab07d66a11b57a0c6ce
<b>sha1:</b>	d0d59ce7c7a5845100e05d899c90267a7c97356a
<b>sha256:</b>	5b17e978c2ca2cf03e4ffff1e4609f2ec98738b1541fa41ba5b67f061e9e2af2
<b>File name:</b>	darkgate.exe

Indicadores de compromisso de artefato malicioso/ analisado	
<b>md5:</b>	fcdc5fa36481d5ace7fa8fc40696ce71
<b>sha1:</b>	dafa96f73f382714fd961f7e399adc2e84f2e751
<b>sha256:</b>	e5ca3a8732a4645de632d0a6edfaf064bdd34a4824102fbc2b328a974350db8f
<b>File name:</b>	651e4a.msi

Indicadores de compromisso de artefato AutoIT	
<b>md5:</b>	78cdadec900811f098b6613495188391
<b>sha1:</b>	b4825b49943f804e5ff9a52d7c661f6c6b345b3f
<b>sha256:</b>	2caa6b5e92ad4c772166860d428d388a4fa376c5adc439b10ee2f045e0a1b003
<b>File name:</b>	files.cab

Indicadores de compromisso de artefato AutoIT	
<b>md5:</b>	856a0bb9b1ebc86a05a2b3367d9cbdd7
<b>sha1:</b>	74da333bcec76419015d7a246b1270cdc1a16e00
<b>sha256:</b>	206042ec2b6bc377296c8b7901ce1a00c393df89e7c4cbbb1b8da1a86a153b67
<b>File name:</b>	65d7c7.msi

Indicadores de compromisso de artefato AutoIT	
<b>md5:</b>	0d813ff082d1f7f3169876e6e58a3de7
<b>sha1:</b>	8bace9b1d0dc3e8d42303f08df2255b67bd07a5b
<b>sha256:</b>	9fd66fbc01bdd8a13ca5a8c41a235c6714e9077a269e65697723c2ab8a775501
<b>File name:</b>	files.cab

Indicadores de compromisso de artefato AutoIT	
<b>md5:</b>	c56b5f0201a3b3de53e561fe76912bfd
<b>sha1:</b>	2a4062e10a5de813f5688221dbeb3f3ff33eb417
<b>sha256:</b>	237d1bca6e056df5bb16a1216a434634109478f882d3b1d58344c801d184f95d
<b>File name:</b>	Autoit3.exe

Indicadores de compromisso de artefato AutoIT	
<b>md5:</b>	b2d5a1369b5b88c18e5123b948683ba8
<b>sha1:</b>	7f537f5045e5e4b77ccb8dcfbd04555b85b11821
<b>sha256:</b>	9a7db0204847d26515ed249f9ed577220326f63a724a2e0fb6bb1d8cd33508a3
<b>File name:</b>	angry_win_0.47_installer.msi

Indicadores de compromisso de artefato AutoIT	
<b>md5:</b>	3cc9a831ae0eb2f227f5f3edd1c55e26
<b>sha1:</b>	014f7fa81d9cbb6c4c6334186e44114815f265ee
<b>sha256:</b>	b6116bcb942a2e13f050417952477e7c8564cc4fd1c4c4b57a67b142b009ab6b
<b>File name:</b>	files.cab

Indicadores de compromisso de artefato AutoIT	
<b>md5:</b>	c56b5f0201a3b3de53e561fe76912bfd
<b>sha1:</b>	2a4062e10a5de813f5688221dbeb3f3ff33eb417
<b>sha256:</b>	237d1bca6e056df5bb16a1216a434634109478f882d3b1d58344c801d184f95d
<b>File name:</b>	Autoit3.exe

Indicadores de compromisso de artefato malicioso/ analisado	
<b>sha256:</b>	8137e72db1c4ef3f375378d62a7dd84c5852a9371edd87f7b2a527609f2553b8

Indicadores de compromisso de artefato malicioso/ analisado	
<b>sha256:</b>	457767a1726bbc1af05175b5a61612a4e1ad29d633e32a887e241acced72a006

Tabela 1 – Indicadores de Compromissos.

## URLs de distribuição e endereços IP C2:

http[:]//80.66.88[.]145
107[.]181.161.200
advancedscanner[.]link
ipadvancedscanner[.]com
185.224.137[.]54
185.11.61[.]65
top[.]advscan[.]com
advanced-ips-scanner[.]com
a4scan[.]com
advanced-ip-scanner[.]com
80.66.88[.]145
107.181.161[.]200

Tabela 2 – Indicadores de Compromissos de Campanhas de Rede

## 6 REFERÊNCIAS

---

- Heimdall *by* ISH Tecnologia
- [Identificação](#) da venda do malware pela ZeroFox
- [Publicação](#) realizada pelo AON sobre DarkGate
- [Publicação](#) do pesquisador OxToxin sobre DarkGate
- [Campanha](#) analisada pela MalwareBytesLabs



heimdall  
security research

A DIVISION OF ISH