BOLETIM DE SEGURANÇA

Campanha SteganoAmor do ator TA558, atacando empresas em todo o mundo

heimdall
security research
A DIVISION OF ISH

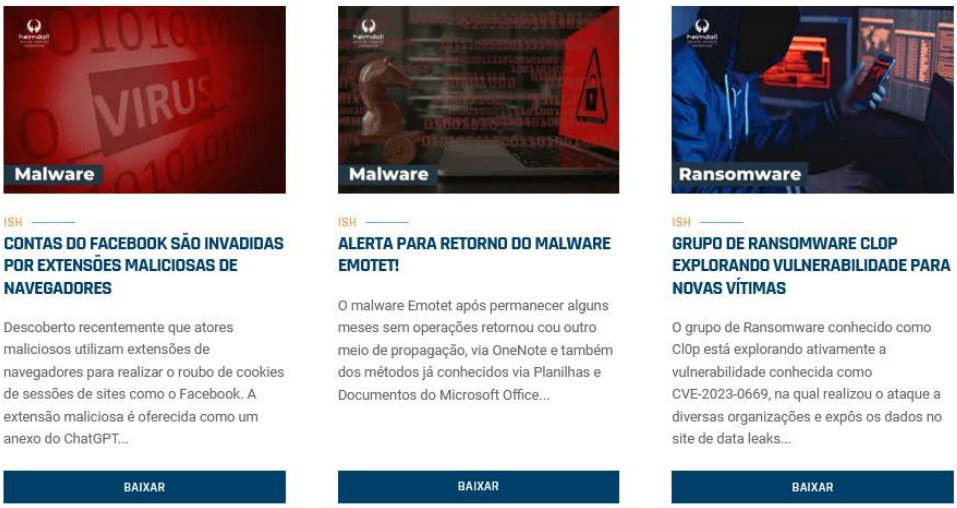
TLP: CLEAR

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

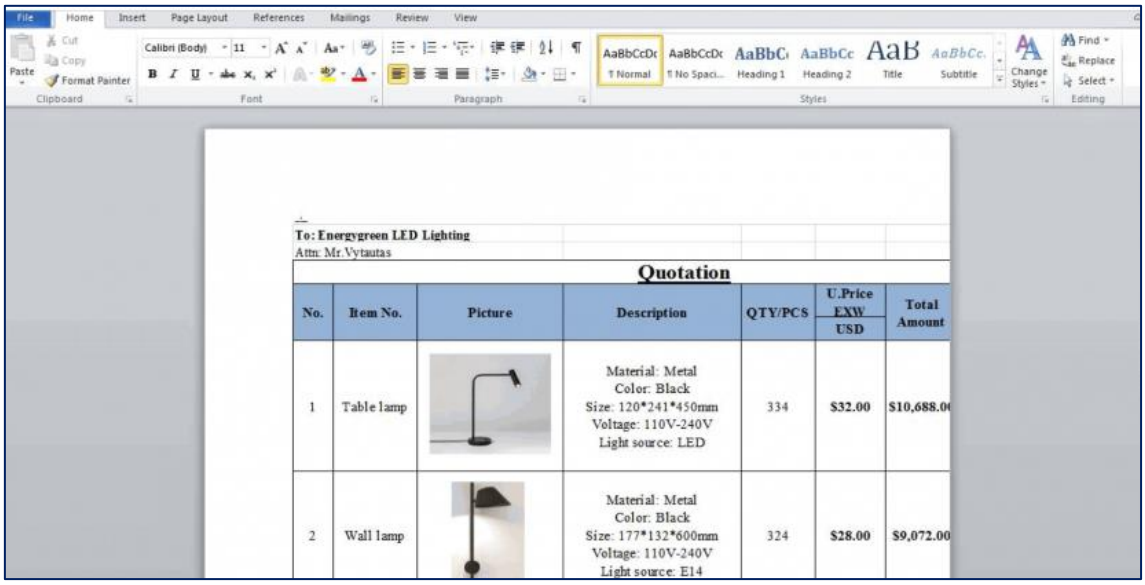
1 SUMÁRIO EXECUTIVO

Pesquisadores de segurança identificaram uma campanha com mais de 300 ataques em todo o mundo, em sua maioria na América Latina, onde segundo os pesquisadores, o Brasil também tem sido alvo dos ataques. A campanha foi atribuíram com ao conhecido grupo de ameaça **TA558**, o nome dado a esta campanha foi "**SteganoAmor**".

O TA558, um grupo de crimes cibernéticos com foco financeiro, mirando principalmente empresas de hotelaria e turismo na **América Latina**, mas também já realizou ataques na América do Norte e Europa Ocidental. Ativo desde 2018, o grupo utiliza extensivamente esteganografia, escondendo códigos maliciosos em imagens e documentos RTF. Curiosamente, muitos desses documentos têm nomes românticos, como "*greatloverstory.vbs*" e "*easytolove.vbs*", o que levou os pesquisadores a apelidarem a campanha de "**SteganoAmor**".

2 DETALHES DA CAMPANHA

A campanha começa com envio de e-mails contendo anexos maliciosos como arquivos Excel e Word, para organizações alvos visando vários setores econômicos e países. A maioria das mensagens de e-mail que encontradas foram enviadas para a América Latina, mas uma percentagem considerável foi dirigida a empresas na Rússia, Roménia, Turquia e alguns outros países.



To: Energygreen LED Lighting
Attn: Mr.Vytautas

Quotation

No.	Item No.	Picture	Description	QTY/PCS	U.Price EXW USD	Total Amount
1	Table lamp		Material: Metal Color: Black Size: 120*241*450mm Voltage: 110V-240V Light source: LED	334	$32.00	$10,688.0
2	Wall lamp		Material: Metal Color: Black Size: 177*132*600mm Voltage: 110V-240V Light source: E14	324	$28.00	$9,072.00

Figura 1 – Exemplo de e-mail utilizado na campanha.

Os e-mails são enviados de servidores SMTP comprometidos para minimizar as chances de as mensagens serem bloqueadas, pois vêm de domínios legítimos.

Ao encontrar uma versão mais antiga do Microsoft Office, o ataque aproveitar-se disso para baixar um script Visual Basic (VBS) de uma fonte legítima ao abrir o arquivo. Esse script é posteriormente ativado para recuperar um arquivo de imagem (JPG) que contém uma carga codificada em base 64.

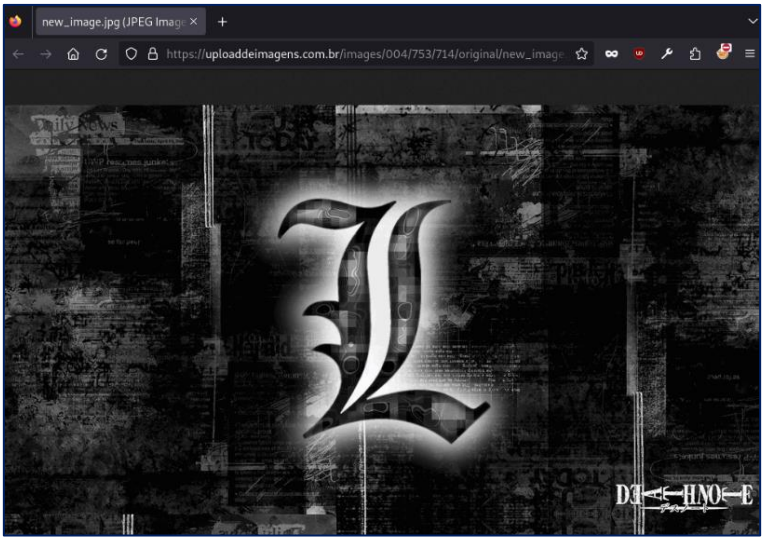


Figura 2 – Imagem esteganográfica usada no ataque.

Uma carga útil de próximo estágio codificada em Base64 escondida dentro da imagem baixada, conforme demonstra imagem abaixo:

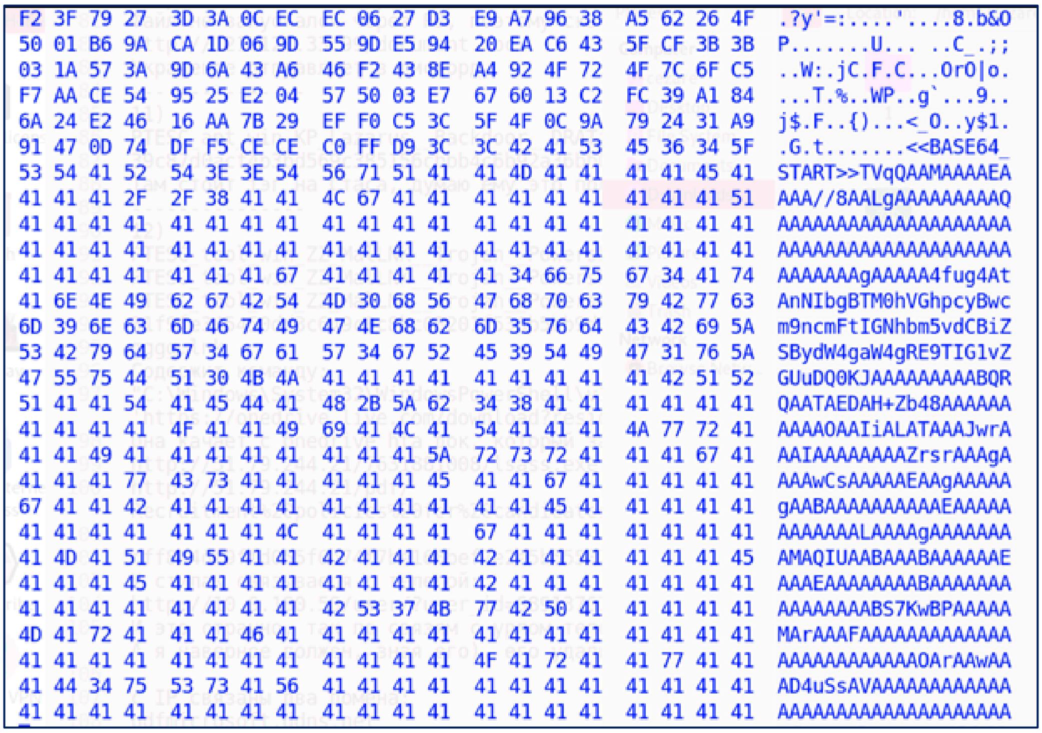


Figura 3 – Carga útil codificada em Base64.

Dentro do script apresentado na imagem, o PowerShell é utilizado para ocultar a carga final, convertendo-a em um executável codificado em base64 e, em seguida, invertendo-o, tudo dentro de um arquivo de texto.

Figura 4 – Código malicioso dentro do arquivo.

Diversas vertentes da cadeia de ataques foram identificadas pela Positive Technologies, abrangendo uma variedade de famílias de malware:

- **AgentTesla**: Funciona como um espião, capturando dados confidenciais como pressionamentos de teclas, informações da área de transferência, além de realizar capturas de tela.
- **FormBook**: Um Infostealer que coleta credenciais de navegadores, captura de tela, registra teclas pressionadas e executa comandos remotos.
- **Remcos**: Oferece controle remoto sobre o sistema comprometido, permitindo a execução de comandos, captura de teclas e até mesmo o acesso à webcam e microfone.
- **LokiBot**: Especializado em roubo de informações como credenciais de login e outros dados sensíveis.
- **Guloader**: Utilizado para distribuir cargas secundárias, frequentemente ocultas para evitar detecção.
- **Snake Keylogger**: Rouba dados ao registrar teclas digitadas, capturar a área de transferência, screenshots e credenciais de navegadores.
- **XWorm**: Um Trojan de acesso remoto que concede controle total sobre o computador infectado.

Esses malwares muitas vezes armazenam suas cargas e scripts em serviços de nuvem legítimos, como o Google Drive, para evitar detecção. As informações roubadas são enviadas para servidores FTP legítimos comprometidos, disfarçando o tráfego como normal.

3 PAÍSES E SETORES ALVOS NA CAMPANHA

Os pesquisadores encontraram um total de mais de 320 ataques direcionados aos seguintes países e setores, o que indica uma ampla campanha, conforme mostra imagem abaixo:

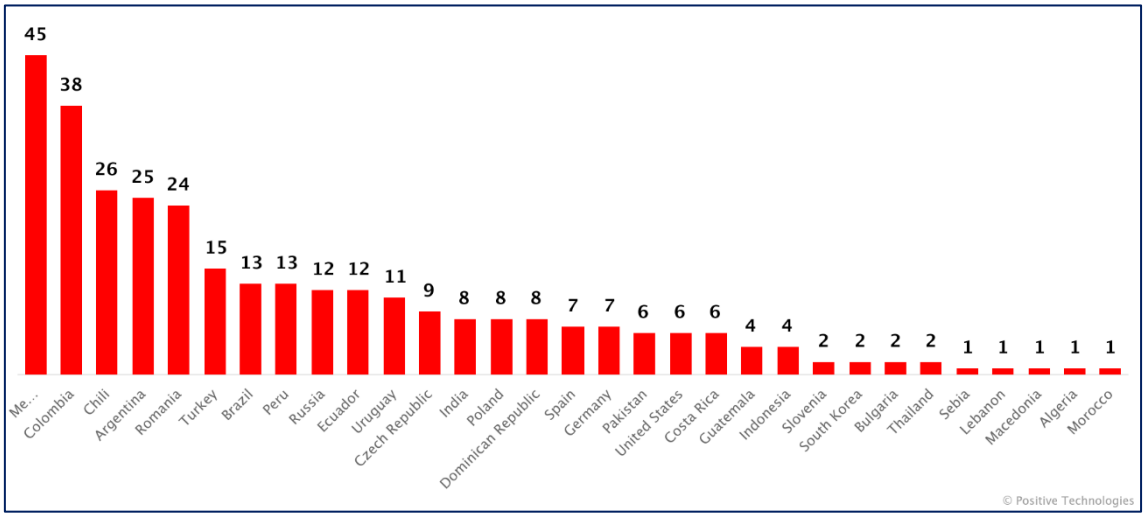


Figura 5 – Distribuição dos ataques por país.

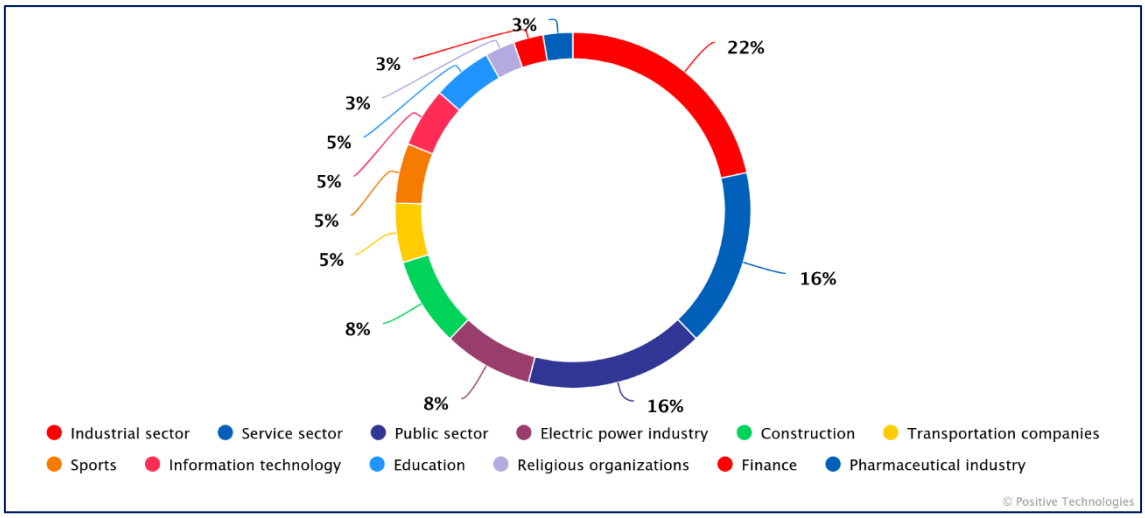


Figura 6 – Distribuição dos ataques por setores.

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:

Treinamento de conscientização

- É essencial conduzir treinamentos regulares de segurança cibernética para funcionários, enfatizando a identificação de e-mails de phishing e práticas seguras de navegação na internet.

Segurança de e-mail robusta

- Implementar medidas de segurança de e-mail para detectar e bloquear tentativas de phishing. Isso pode incluir o uso de ferramentas de filtragem de e-mail e anti-phishing que ajudam a identificar e isolar e-mails suspeitos antes que eles alcancem os usuários finais.

Atualização e patches de segurança

- Manter todos os sistemas e softwares atualizados com os patches de segurança mais recentes é crucial para proteger contra vulnerabilidades conhecidas que podem ser exploradas por malwares, frequentemente usado pelo TA558.

Antivírus e sistemas de detecção de intrusão

- Usar software antivírus e sistemas de detecção de intrusão para identificar e prevenir infecções por malware. Essas ferramentas podem detectar atividades maliciosas no sistema e ajudar a mitigar os danos rapidamente.

Gestão de anexos e links em e-mails

Adotar políticas rigorosas para o manuseio de anexos e links em e-mails, especialmente de remetentes desconhecidos. Isto é particularmente importante, pois o TA558 tem utilizado links maliciosos e anexos de documentos para implantar malware.

Além disso, as organizações devem estar atentas a técnicas específicas usadas pelo TA558, como o uso de documentos do Office e PowerPoint com macros maliciosas e a exploração de vulnerabilidades conhecidas como CVE-2017-11882.

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:	4c7bdc42ec5df40146a73fef5af4928b
sha1:	08b7d3b19ee002fc1977170c94f26a412dcd3787
sha256:	6ca1bff32ddd346f959911e8aedcf0bbe3a3da18a143baa3c44d1b625ef1eb1f
File name:	4c7bdc42ec5df40146a73fef5af4928b.docx

Indicadores de compromisso do artefato	
md5:	4a6c8b75271dfb2968fb511984fcdf56
sha1:	607a5d42b94aa5362857f893f5ff12d8fe6b7dcb
sha256:	cd1c9fad93fdc00b3d2b34bb65d84029c5a8529b7eba10b4922b503dca449c74
File name:	cd1c9fad93fdc00b3d2b34bb65d84029c5a8529b7eba10b4922b503dca449c74.xls

Indicadores de compromisso do artefato	
md5:	20684d36620f825c2997a99f86fbaf7a
sha1:	1bdeab2b6857e99af6d67c1038e793710423607a
sha256:	05dcad5146ced653ac37a38ac3088de9542fc2773c994ceb1e32dc706261c193
File name:	05dcad5146ced653ac37a38ac3088de9542fc2773c994ceb1e32dc706261c193.xls

Indicadores de compromisso do artefato	
md5:	d53f7e00291f84524a082751b60402ee
sha1:	0c806d77241b6b7fba72cf608fe619db86c62194
sha256:	ffcc528cab820f16da6b2e9210adf688c291455fc0c1d47e87fda017f8e16883
File name:	boominginternationallythetotalfileworkstounderstandhowimporatntto_

Indicadores de compromisso do artefato	
md5:	12ce424e2d7bf60c86e697c97109146f
sha1:	30ba7c406754335058fd1c59002318d5157df9ae
sha256:	ff1c6fe051be3018e58f56d19ccad79c76be7c7de1054ccc2948996ba068544f
File name:	mecrazylovertounderstandhowimportanteaturesneedtoaddinsideof

Indicadores de compromisso do artefato	
md5:	5496804597a1bf4beb89256c24c27c35
sha1:	5a39a8e9f872de1207e49a20b4baf2eaf156cb35
sha256:	fe46f0ed67fd82da0561fb894b8928b2538185173b2dfa0dd543daead2d026ad
File name:	fe46f0ed67fd82da0561fb894b8928b2538185173b2dfa0dd543daead2d026ad.rtf

Indicadores de compromisso do artefato	
md5:	0df35a6bc957bd586d9e3931d5fe7a22
sha1:	cf1a9a7997fcfda446f396cd915dc7ac4c7d878f
sha256:	fdaba17c9e898ed20233a853be28ccb5ff9410a623ab42f5e330079a2b7337f6

File name:	tedloverspointtothisweekforentirepurposetoarrangethelovertounderstand

Indicadores de compromisso do artefato	
md5:	b39ac38fa0a7dd2bd9786c3944e087fa
sha1:	761926f3ea3b5b68ac0749ff965aba15b67690d1
sha256:	fc383ae9ae43ca53b0cea754c85e4cca4c978ccd45f4fdc1a19ce3f2c6857bad
File name:	po3495954.xls

Indicadores de compromisso do artefato	
md5:	e79c9e9198572695f518a70c66afed2f
sha1:	4337db458d185cc465b804e57cd550cfb64dafcb
sha256:	28079328abb78e6503a68b6097c7da8c936474e50e42b6143d89658890c53d0b
File name:	Fatura ödeme.docx

Indicadores de compromisso do artefato	
md5:	646ce6ec3effd4b9d7cd93c656cfdbdf
sha1:	3f2affe56ff8af95727a64faf82ff8c99d3607ee
sha256:	f9e336279a1e2bf97ef4c8179b3507c4acda345c388695d766ec5f423be22577
File name:	f9e336279a1e2bf97ef4c8179b3507c4acda345c388695d766ec5f423be22577.rar

Indicadores de compromisso do artefato	
md5:	88c9646797eef80e9184085d8ce32662
sha1:	1f07b17cac8d2327e1b16c3114dcec27407a3cf9
sha256:	f229b3725dbe9bc2b555daac400a1549cc6439d1a46e20a41578f42a2bf4c70a
File name:	Mpglfl.exe

Indicadores de compromisso do artefato	
md5:	33bdebc8c9eb9374b33c357ebb01fbd0
sha1:	48defa74814d2744c7cf4cd3731f6dd91484f1d2
sha256:	f0424ecae14b1eee4a874f7c013358221fc80468164de6e88ea7d057eca7e0c6
File name:	f0424ecae14b1eee4a874f7c013358221fc80468164de6e88ea7d057eca7e0c6.rtf

Indicadores de compromisso do artefato	
md5:	040bf1a02d4caa5a7842f5c721ebe8e3
sha1:	d57c9ec3f6e103d79f37763f08ab4d400d9c88a7
sha256:	efd5d48c7e7c986e7af1a716eed388b3c2832f3fdb73700642601467e271af31
File name:	FORECAST-SAFETY HELMET New Order Request.docx

Indicadores de compromisso do artefato	
md5:	6e3537a1bbd79ea9cc4dd5de11f59dae
sha1:	954387bc240bcbb21b6c80509da81df93a2b4d3c
sha256:	b8b90bdda88d3417350529e203f593ed62a737639c8076c373e6135859a086e2
File name:	b8b90bdda88d3417350529e203f593ed62a737639c8076c373e6135859a086e2.doc

Indicadores de compromisso do artefato	
md5:	8f2f4b5339a20be2102dc14258a30058
sha1:	171190414bc88f58d4e0c67129a22c65973ce943
sha256:	b7160e3400ac72ba74a94525cf2061f10763bac093d96ce651300288ea2f1070

File name:	PO.xls

Indicadores de compromisso do artefato	
md5:	6f05888f255f6383694853973f8007fa
sha1:	48efdbb41f2a724b2d158b32f7aa34fb25d9c658
sha256:	b2baf74a7ee97999730fe785548643f3c55839c06837eff7f24617131668d955
File name:	Unbezahlte Rechnung Nr.12417.xls

Indicadores de compromisso do artefato	
md5:	98b8bb7c10d46e969ec3def1fc4409b4
sha1:	db48b90b3c3fbc58b90a08b74ac948c25a15c0a0
sha256:	b162b45839d7c3b61457f814b0c317226ceeea22dc1a286283d114d1d835eb41
File name:	b162b45839d7c3b61457f814b0c317226ceeea22dc1a286283d114d1d835eb41.bin.rtf

Indicadores de compromisso do artefato	
md5:	d04a984c872760499ec9537c512d3766
sha1:	cb210c13c9f94e0e2273cf50740a3d32b08d8fda
sha256:	af7b9b3a213b28e752d3425e69d3874fa94d57ddf8cf57ab3899f6bdc532ee8e
File name:	HSBC Payment Advice.xls

Indicadores de compromisso do artefato	
md5:	d3a71be05307fe483a8cbf2ced9824b3
sha1:	c7be6c8c83b1d019735464a96460c452834b54dd
sha256:	a9bd81ae5d703b95c1a06f84802d01a875b11a9e303b31f0cc15786fd5ccad33
File name:	iwanttoseeitsgreatideatounderstand.doc

Indicadores de compromisso do artefato	
md5:	0d6534a2466c7ee9640c194b4bc62545
sha1:	6c99895b6cc25610f7d882693a06f7762eac0b9b
sha256:	a86c6e2995c830758d9e873844bd89ff739ee366e78d2c2457ca75b67a79cbb5
File name:	266898627

Indicadores de compromisso do artefato	
md5:	9043647d2c71640d02d1b5a5b5ed938d
sha1:	880cdae437a21e8d7d45be18b0135aaf32146893
sha256:	a59d04040da8d05a2c51ab2c1247b3b2621dc5f092fada0f5189cb1a3858e24c
File name:	266359266

Indicadores de compromisso do artefato	
md5:	e41ef98b056ef91945c17544fb5e30dd
sha1:	557f7ae7b7382c2bc06db09f7cb07f640332238a
sha256:	a3a20a621de2a22a262e287713910a92d6cd9212af1d30e8a5a167f8a91f14c4
File name:	a3a20a621de2a22a262e287713910a92d6cd9212af1d30e8a5a167f8a91f14c4

Indicadores de compromisso do artefato	
md5:	921f329135f8544363dbf20114e594af
sha1:	95b74f7267867cf7f538876428cff90c2430ce6d
sha256:	a306c3cb8e8b5448ee4a9bc49a3b671b10d76172010d2bb5da629f5371943029

File name:	Quotation.docx

Indicadores de compromisso do artefato	
md5:	0cba0d555503e54b720c52cb1f37a3dd
sha1:	5301aec910164eda6b9b36ba04a51211d038786e
sha256:	a23b9d9d263079d79dbec3794490c4917141f4dd385ce136fac2f58c0f9ae5ac
File name:	a23b9d9d263079d79dbec3794490c4917141f4dd385ce136fac2f58c0f9ae5ac.rtf

Indicadores de compromisso do artefato	
md5:	2707b9ed82b1deda4cb0ce3cc3e727d3
sha1:	cc9400861fea3deee8815eb34b7f5879fd6ca3ab
sha256:	a1d323166349f499aa796148c0120f89d3a0946abdf74f0dc045c5641b2ab2d3
File name:	known-sample2.xls

Indicadores de compromisso do artefato	
md5:	a177f5a4992ac9aab718f15c71f2b0e4
sha1:	a4309c6c02bb320784c5952bf900eb2cd43b6ecf
sha256:	91f7d692760bbadb48882e8a8d8abe9e6890bd4d5b735fad22b3247693da834e
File name:	Updated Order.docx

Indicadores de compromisso do artefato	
md5:	0ec85d950d76c39348e38a342058f9a1
sha1:	c00a137d85855be8c462f835de67201124de62a1
sha256:	a077a9f97badfc285269999a22fa67ffaad234bf365486a66167bc53457d7663
File name:	0ec85d950d76c39348e38a342058f9a1.docx

Indicadores de compromisso do artefato	
md5:	98d2580289f8c25658225ac92aaeb179
sha1:	0046a5cf40bafa768b5afa282b91c63dd9fddf5c
sha256:	9dbd6f1fb0be8bd4a000ab35f4ab5c9505bf5ec72a17ca1223d7ad240d974423
File name:	iamgreatlovertounderstandtheprcess.doc

Indicadores de compromisso do artefato	
md5:	e44aa3fc8915966c0164277654982012
sha1:	dfba0231d1991f3f4e702d44a4c90598b99a2e9b
sha256:	9caeaefa5ecb508895fef48764dc689f49dd8ad9f7e4de9e52202f1c1db101e1
File name:	9caeaefa5ecb508895fef48764dc689f49dd8ad9f7e4de9e52202f1c1db101e1.xlsx

Indicadores de compromisso do artefato	
md5:	5f9cc6a878cf235dae2033762aa0d2d9
sha1:	9befcfe5eb0f5fda18fed13ac4906eae3b702387
sha256:	99813dd920b37531d7e9dac681fc90efcb9e8996b927e3202e14028cf5e32385
File name:	266752112

Indicadores de compromisso do artefato	
md5:	72b66b3acf7f916a27a2c38984461fe0
sha1:	fa05f64345f74503e8d9ee1ada145942109c8aa0
sha256:	96569d96ffe599a1a7857f454ea1d6181c39941c29b72f28a5427570bb1558af

File name:	6DA70000

Indicadores de compromisso do artefato	
md5:	485f8284359ac9dccef395ccaa38e73d
sha1:	63b4c7daf5d4f821b660cf07733f067ac87b3662
sha256:	9388a04aa9b347704d4fb9b07035a640fb0f4a07e4b2870a3eb0b4bc4abdd007
File name:	INQUIRY 00103122023.docx

Indicadores de compromisso do artefato	
md5:	a01fcd2a71ac256583f9f1b0d1bb5cdf
sha1:	7636aaf9e6186f81da27b39031504aaf33546aea
sha256:	9236af505a3ebbb408b4cdd0f8650309951764d6c0234ee75bb8d22d8b44a08c
File name:	payload_1.doc

Indicadores de compromisso do artefato	
md5:	45b64e21f4ef4a9248ca77fe18af7b25
sha1:	7eb41cac06080bf49c46725455aea2f938581ce1
sha256:	91e6b7422ba81d359bb76c1ead103600b6258d6b53ea511c11f7295192573dc9
File name:	

Indicadores de compromisso do artefato	
md5:	c597f50730816c8a2b1e8a9952a9bcdb
sha1:	a7382690fc0c843dd101b97b2b2a33d82912a88a
sha256:	91d02bfc9a8699fea8f447158a67d90af2f5cf62b024b283611d17c9f5fc8567
File name:	91d02bfc9a8699fea8f447158a67d90af2f5cf62b024b283611d17c9f5fc8567.rtf

Indicadores de compromisso do artefato	
md5:	59ec1a55c20b6464ebee41b126e5eb87
sha1:	35ec7d9a0a0b6914fe636ba89a3ad059ed881051
sha256:	8e99014f6cf2ab5fff2b0b86c2aef86827f69f7cd2d443d82c9bbde1c0ed87e8
File name:	

Indicadores de compromisso do artefato	
md5:	36a36c711ac6aa0fdaaaaee1cd39763c
sha1:	665270dd573f8486a68b8a9082d71b21fca952ac
sha256:	8968fb7e81053d652558b77a2048f5dbdc9b3ba2e8835acddc5c2c213ef979d9
File name:	brwoserdeletedentirehistoryfromthepcforclean.doc

Indicadores de compromisso do artefato	
md5:	1f677f128897e4e490351e140776a44a
sha1:	363cbb65b86e443f24de3d4915db01208217c08c
sha256:	41e92c70e0cfad3d8a15b25c9abbc79a3145444ec2c589881b46116ccb7b0a7f
File name:	41e92c70e0cfad3d8a15b25c9abbc79a3145444ec2c589881b46116ccb7b0a7f.rtf

Indicadores de compromisso do artefato	
md5:	755932e4a5dd0262ac2b91a3f28e09eb
sha1:	36a98688e0d50e0584034daa45565b75905de044
sha256:	4146aa473e4605091ab178f61e40782bda93cfbba733f52ee02a6b51fa0f052e

File name:	tobefrankiloveyousoomuchmybabygirltoseeyoualottounderstand.doc

Indicadores de compromisso do artefato	
md5:	ba76cccebe5adfdc669e933b5fc320e7
sha1:	7457a05e415855131efd3a4c1bfda45a9051a656
sha256:	3f4f5e4f1b608b471db6433607ea0b223c31df06e35a740572747e9a1cee54b3
File name:	htmlbrowserhistorydeletedbymictosfotEdge.Doc

Indicadores de compromisso do artefato	
md5:	86ffb0a3da748e5fe5f7dfa4bb2bfcd6
sha1:	8eab0679cfb78fe905758bed258de9f454d6a65e
sha256:	3d3dbaf0766de69b7f4655933106d1ed0282a5ec650c987e31fb3e0a1e0f195d
File name:	PO1876.xls

Indicadores de compromisso do artefato	
md5:	26570b685186f148d866f342f94d04b5
sha1:	46d5d6e37c2062c8c7aef94dca143520d4be42b8
sha256:	3cc2f066ba77c5d0468f77580957ce0d872961f8803bd9dae47ee65a8088b004
File name:	RFQ No. PO414501.xla

Indicadores de compromisso do artefato	
md5:	cb38fffe4cecba910dd0817a0e755f11
sha1:	248968f14c1706a105f86ed9da4cdb48a98535e0
sha256:	3b8ec0e9542ec0bddb9ee64b4644c65c069f1c03a505e7079fd3ff209ff5045b
File name:	266344114

Indicadores de compromisso do artefato	
md5:	4b8d9718182adc5a816e871c94e893c8
sha1:	b4738338f23c754a889f88a3de30fa7341b2de76
sha256:	3b89a9f5f315f37ec110ec2e59c40e9635841115a73bb031edcbe7d059904ae2
File name:	3b89a9f5f315f37ec110ec2e59c40e9635841115a73bb031edcbe7d059904ae2.rtf

Indicadores de compromisso do artefato	
md5:	0cd0b71b219419b688ecd6599223639a
sha1:	fde7e33898b73304755f1cff8578139f34246e23
sha256:	3a23b616a5944735ffa156ebfba3fcf8debec466c00687a52ecdbde03b2bd94a
File name:	Quotation.xls

Indicadores de compromisso do artefato	
md5:	10a0a845587723ca7a0f48d013e93d9e
sha1:	17d8ea8de47cf645f4f922a9e601e74e3705bfcf
sha256:	39eb5f6f12c6556ab7556dfc5684e430323ff1768d305f527538615b55b884b8
File name:	Mit freundlichen Bank detail.docx

Indicadores de compromisso do artefato	
md5:	ad19c30e8fc0f89004a1f960b477707f
sha1:	0bb59500525d0b45c506c7b4fab6c1d905ee3280
sha256:	395694b99ce0310e2aa9e6b96f479c36956af254b047c959a022c2b1fef2d6c6

File name:	256428561

Indicadores de compromisso do artefato	
md5:	fe1947022cd5ff9d3ef2f267f323833b
sha1:	ca07d2d6c63dad12362bd6b5576721e3426156ae
sha256:	379bdcb7512aedd9bb87d875d66281766a478b2288f1074b95d938589059d4f8
File name:	Satın Alma Siparişi -VAPTECH JSC.xls

Indicadores de compromisso do artefato	
md5:	3a676a14c0aa582a465032b971ca23f5
sha1:	04b12227d6b22ed562005d126cd7e3366c4fe966
sha256:	3688f05556a136fe094de5cb1888eac2a579525f72cd027e19738582ed40c283
File name:	NEW ORDER.xls

Indicadores de compromisso do artefato	
md5:	e567a41dabaf821c0bc51aff2925c190
sha1:	761fe57c2da0aa95562369e67370748239e390db
sha256:	34d4f41be41415d251e917eec848e3a0e93a741ef5ac3d17e2781597c6d947a9
File name:	payload_1.doc

Indicadores de compromisso do artefato	
md5:	18f15cd6a792ea9a0a5d835e9e9e5c89
sha1:	5d9f70fd761854f72c719aad591f8a29d70d5300
sha256:	317823955933fb40757674275b08eb58d03956459a0c2d30cb14b5edaa557c2b
File name:	payload_1.doc

Indicadores de compromisso do artefato	
md5:	01984a8dda890f0ed6dfd9b6b12fbd23
sha1:	9abd358ab00de031588bbe3d4cfbfb02beb3a00c
sha256:	2f346530bbcfd52b48cc589e1ba8f42ac72eae31ed9aa0b0e20ec7df0cac3bf6
File name:	267465072

Indicadores de compromisso do artefato	
md5:	55fa849c3fa213c1d7127af40c569a06
sha1:	d3bcc82d43fd4accc211fbbba5805c5c314d9254
sha256:	2a8e81ea949501a0c65786800d080f8162e56e7a6f988231097acebbf86a7b61
File name:	2a8e81ea949501a0c65786800d080f8162e56e7a6f988231097acebbf86a7b61

Indicadores de compromisso do artefato	
md5:	f59d97797189676917d0b462a080fd29
sha1:	a660ab84283b72f7a371aa806092800a0af1c134
sha256:	2a3626fa590b72f5a372351b1a8e18a524f356b1499f8a08af326c67692217cd
File name:	sw-O2024-Invoice.docx

Indicadores de compromisso do artefato	
md5:	9653583758a6bed24ef3196424892166
sha1:	87e7e8fd6e6b95591edde3ceefa7ca3ae3e857e6
sha256:	1d8afbb50c3e46ce4311d51bb1af9fbcace0f3db9b4ddf3a92f2e6e4fa7c6d1d

File name:	1d8afbb50c3e46ce4311d51bb1af9fbcace0f3db9b4ddf3a92f2e6e4fa7c6d1d.rtf

Indicadores de compromisso do artefato	
md5:	263e05601d520fc6dddae63a2346eca6
sha1:	55f96d85611d46d948370b68dd300b0fc9042f2b
sha256:	19a775bd69ce741a815e6f67b3b78d04fad87a296ed2515e88b1ad3fc5a74aae
File name:	266752230

Indicadores de compromisso do artefato	
md5:	a77330743abb7fea71dbc33a122b3c09
sha1:	6b7c0946aa8c00ea239b73eba3baafd559aa7683
sha256:	164e8075fd8029e9c27525933f62ae9d1aedce53729b58630935a7c2299b350a
File name:	Export Documents.xls

Indicadores de compromisso do artefato	
md5:	afd58c071d6a783e11854b9efa544840
sha1:	30a6538dbede15967e30c0c20bbfa6164229c7fc
sha256:	13330cf96be68f9c1058a2608ef46ae54d9af561790a2e4b6428b076d40f457e
File name:	E38931D7.doc

Indicadores de compromisso do artefato	
md5:	a4a7d9d368757b4d491b8b295abfd16f
sha1:	89bb7cf606ede494dab8c89282ea399418f536f7
sha256:	12047ca7ecfe6caf4a9798565ade481d1a1c46f7d1aa09b6576b11a36b431547
File name:	RTFM

Indicadores de compromisso do artefato	
md5:	612413293cd0c309075ebf2898115316
sha1:	53b5ab29ad6bb922960fc7614a2643b8b4277a05
sha256:	0c28aedb85b82641bdbe7270293a97f440dbcfa14489b1348fa89ce0ca331896
File name:	gsforgreatthingshappenedaroundtheworldtofocusfornewthingstodesign.doc

Indicadores de compromisso do artefato	
md5:	7193e486093ab597825062dd2e1bbe4b
sha1:	9cc536e983081790eabb19cf872dfc612e39aeb1
sha256:	09d5e042a8c569bc785d4937bf4b07f53897c37f5d91304f2a69ed18ec60d7ef
File name:	wAZNo

Indicadores de compromisso do artefato	
md5:	b7fbea603526450f9f196f0351b411d2
sha1:	69cec4e11ed336b0c5bd4d5d39ccf49c96ad7823
sha256:	06e152dd7b3d5488f65efe376708f9fdc8f5b1f061f2586607a142d6aff8fc3d
File name:	b7fbea603526450f9f196f0351b411d2.docx

Indicadores de compromisso do artefato	
md5:	23d984b56442dc4d69c773d3e7e7a8d8
sha1:	ba1d5792f37d858c54df890e48bdb5c438821d96
sha256:	03905ce2b853ebb6341c53ce261752613d067720491765fee7be8875d941cf82

File name:	standwhyimportanttodeleteentirecachecookiehistoryeverythingfromthepc.doc

Indicadores de compromisso do artefato	
md5:	f9a4a421230c941005f983604a619ef6
sha1:	dc8a3f1164bf81c9aa872012978ecba503c0d1c2
sha256:	036be40c38dfe9b01a9830dc58c05a29ba0c7667f3913257e84c7db54ff32db5
File name:	Reports Remit03.xls

Indicadores de compromisso do artefato	
md5:	a126d8e25e0d57c17c815713b389ee34
sha1:	f879369a4da547c9778025ebeba3b58e28372f8e
sha256:	ee5c4b17cd1da34f6ad2d47de7bf8fad000705086c34243cc0d36a15e1dfb903
File name:	B01C175B.doc

Indicadores de compromisso do artefato	
md5:	ec96a9fd53dea71b91467846c09a2322
sha1:	6ef72c533964b464567212a63a1c28919fdc147b
sha256:	b9195453fdb779b9afeb2178c7b8ff8ac2769afa52b9f6ae10ba4915fba77e5c
File name:	b9195453fdb779b9afeb2178c7b8ff8ac2769afa52b9f6ae10ba4915fba77e5c.xls

Indicadores de compromisso do artefato	
md5:	de81ca904b88240d1bdf3e6ce5211367
sha1:	04b96d917496857a4e5cafd042e1594323437a5b
sha256:	ec5062b6c5c6648b188b29b28741d4911a36986ec5adccad8ecffa5e8b41734b
File name:	ec5062b6c5c6648b188b29b28741d4911a36986ec5adccad8ecffa5e8b41734b.xlsx

Indicadores de compromisso do artefato	
md5:	eba7cc1d50adab9015ecee5ae3512fc5
sha1:	6c90360abc9605eaa09a630217f14961c30ac70a
sha256:	54376ee15cca7c6cdecc27b701b85bdd2aa618fe8158a453d65030425154299a
File name:	Lista de productos 2.docx

Indicadores de compromisso do artefato	
md5:	6de35c22ca3f026a6a645fc9fda40565
sha1:	252a6d49a0d9096e8c48c11d7c9a934681e55f6a
sha256:	e9d8f145cf7e0745a6eb448fe68cb774fb5549440218fae3be937600b7b1bc96
File name:	FACTURA041223.docx

Indicadores de compromisso do artefato	
md5:	e7b1dab5d64b8e37ab2c8b0a05fd486c
sha1:	5ae4d3a7dec17b9740d4573e8f1014769e683f79
sha256:	fc8d8e349b245c33b43169523d6d8ebbc617f07d3ec592bc71eccba272a53bed
File name:	sweetkissigivenheronneckandfacetoget.doc

Indicadores de compromisso do artefato	
md5:	c86f12255fabf8b223f2aca753727dfa
sha1:	33939e398901764dd5ecd0cc567f0ff5a89029d9
sha256:	e60d9091fb659fe00b1c4a25825e82d9607fedfe48e9c46a52ccca782cfcf69f

File name:	e60d9091fb659fe00b1c4a25825e82d9607fedfe48e9c46a52ccca782cfcf69f.rtf

Indicadores de compromisso do artefato	
md5:	11132e1c20a4b54f5d04e70ceead9b6a
sha1:	2b8e2c6709e2f3920941384d492cbd7b478ac3bc
sha256:	e07f65fd99a36e8d930a40b95ee09203034e242cb3ba4058496903fde05a6231
File name:	Unconfirmed 233941.crdownload

Indicadores de compromisso do artefato	
md5:	9e8948e8a2ee90bfcc000ba2246e87d2
sha1:	f7cf182890f3321eaecbadb9d21ce31bc7f0e722
sha256:	df57d5c5e318a81ce2ed7924741abb127f2955d2ec0826c83663bd0137c9e269
File name:	bJazC

Indicadores de compromisso do artefato	
md5:	2d6edf232ef2f4e9ac72de52b4b4efa5
sha1:	2bbfb909e4e3bb1a1518e973afec5b587b59e426
sha256:	dd94c4c0dd46a40cb71f1b59b079577c8a4f6e4a1df88533d7edfea19099729c
File name:	Package.xls

Indicadores de compromisso do artefato	
md5:	9569c625fe07176dfe4f65e27891c8a5
sha1:	a5d786f8d9ad0fe1ffbd6a8b00950f96d82420bf
sha256:	dd281ccd017d05af98701f22870d30ad99b89c64d68962c60b93147b187f9524
File name:	Swift MT10348565.xls

Indicadores de compromisso do artefato	
md5:	ccca2007f5e72e8ed7bde35eff192a59
sha1:	12aa02703b0f69bd6e2084405b3d1f0c06c85f84
sha256:	dad62d3203e96eb88d25d3f0969c6289e64e7bf0c8135e7b9f468a8ea9ff3206
File name:	payload_1.doc

Indicadores de compromisso do artefato	
md5:	a5c477fe361014b945b4ca609f992e62
sha1:	9293c09804ff0e14fa9112b2138f8aa1c1d7ad11
sha256:	d9e24ffb33ee9ed68cae4ec00160898b6ccc4f20ee75d5cd1e7dae6d56ba2e51
File name:	payload_1.doc

Indicadores de compromisso do artefato	
md5:	0c5b1cce06e972bb77b1990284688981
sha1:	5fb1ce62fa6753a9b217e7e9e7c5fea780b1e571
sha256:	d5e8ac20bd384b8c4f2b71d6963d504a9c546ff9427ac12157b00da7fe6a9734
File name:	youbecomealovertogetredayforthenewonetogetforme.doc

Indicadores de compromisso do artefato	
md5:	07c3147caa9efaee6d548eba9eef219e
sha1:	f537c9fd4ab19a1c2a65d002fb61b60f5820f8da
sha256:	d306c83b6688dda1592b7c63c7f45299f5ccb2b8b75a6df990b13adf67f0b272

File name:	267160957

Indicadores de compromisso do artefato	
md5:	6d243110db79ee1eb0438a2e7b96ec55
sha1:	4bcc2b5b1c3a8d5ab5f81b7f249480da91b1eccd
sha256:	cdfb07f5c1848d62f49dbc2497f8d05dce04bdc1b3d4ea264b40eeec03b8aa5a
File name:	heissocutetounderstandhowimaandallsheis.doc

Indicadores de compromisso do artefato	
md5:	bc163cddee2ebc25e3eeb9fd62e4ebb1
sha1:	aed1d5b7bffec047b22152fa4cf7e601c8ba963f
sha256:	caf61fe47dfac15c2c4e0f6db57bd60e752a14b3fbaa2b705ff4b4c11f9e32d2
File name:	agirlwithallmyheartstillalsoiloveheralotkissyou.doc

Indicadores de compromisso do artefato	
md5:	cae8bb9d33e2340998ba5f75ad37f803
sha1:	75e142060680509acade4921ea417e1d438a34fd
sha256:	aa48be12373eee7adb43270e7adde9a854875ceebd5c267fa6bbb79e91ce2030
File name:	inf1.rtf

Indicadores de compromisso do artefato	
md5:	07c147c508668defb1817d2e187ec9b2
sha1:	e2830040a42c15c3825c2ff5ed7c96f3e7a14dc1
sha256:	cabeae35ddaadc9b285400eef5fa6b08ca978ebab1d7dcc386725d522e44e785
File name:	myheartmylovemybabygirlsheismyall.doc

Indicadores de compromisso do artefato	
md5:	ca93ad9d9887663ed1afc2197b775268
sha1:	017bb90012dfa9fd9a6a05efd01d1d929e411039
sha256:	3a1b13e80cfd6e053f5a605e531c17a936a33fc5c5467e40be5a8845a2d2dbcb
File name:	PO-5299.xls

Indicadores de compromisso do artefato	
md5:	984658d36ffed26548d1c625a6f4718c
sha1:	5787b635711b51cffb3399ef069f58683a18e9c8
sha256:	c8acfc0a8a5144d6472d6761ed175a855802e625359eb33fae7962d087908131
File name:	meandmyloverisverygoodrelationshopilove.doc

Indicadores de compromisso do artefato	
md5:	8129abc7b545b3e42fee6d8b0f719de3
sha1:	1396c25a417e8fb7cf4e6b72899688b9f6ea8329
sha256:	c4d6e9d13089b15a952d9bf10fe34c7fdc36ccfa00b61039cc9c81cdc7b84686
File name:	greatlovertounderstandhowmuchsheis.doc

Indicadores de compromisso do artefato	
md5:	e6f76b89356f767c1e4579b115621d8a
sha1:	d316f5418950945761c24fb92a6b8e017c53010c
sha256:	c39e6397fdcff66da2ebb9fc2a8c54671a3706e9e15cdd5e50c5009b205469bc

File name:	c39e6397fdcff66da2ebb9fc2a8c54671a3706e9e15cdd5e50c5009b205469bc.rtf

Indicadores de compromisso do artefato	
md5:	36cb1d700227ba18a13425d53c4f448f
sha1:	9a1c421150c716aa9eb24944c53b42f3d04faace
sha256:	c2d92f57c551932f68c704db32918b01eedef76decd521782ddbcc1aa6087588
File name:	c2d92f57c551932f68c704db32918b01eedef76decd521782ddbcc1aa6087588.xlsx

Indicadores de compromisso do artefato	
md5:	9282088d06c3ef7436a8f8fbfdbed13f
sha1:	53122c78ed663ad84714ba55e6690934ab05077c
sha256:	bf33684f4ac18e2823d8c7c7ad7370baabd4c4b57506ed620cddda203512eed8
File name:	omysweetheartumygirlwhichireallywnat.doc

Indicadores de compromisso do artefato	
md5:	61ebc536a8018c94dd5ec0dbe911dce1
sha1:	f80549805bbdd9a62872365be4dc8aceaa71340e
sha256:	be1173550910a40bd03c78f0f9aba5a8572e43b79fde162ffce521d833d9b8bb
File name:	playingfamewithmeshewantihavetoworkonthegamelover.doc

Indicadores de compromisso do artefato	
md5:	4d8bf77e9def007fd900684dc886c102
sha1:	2c070e8123357f94dc0cfaf584c787c0793760c6
sha256:	bdc926e8bfffface9dfd885a03488e675f1633519fe30181d013a3e1f0f33202a
File name:	ABFA7540.doc

Indicadores de compromisso do artefato	
md5:	a4ce1a6aa5c3545900c08f314c057eb2
sha1:	a6d68f4ea448e4945788d47d434e697508d3728d
sha256:	bd9f2e8e17f8a223ba9d004fa8cc6bdf2a5a1abb54cb565ca166996cf7240dbb
File name:	a4ce1a6aa5c3545900c08f314c057eb2.file

Indicadores de compromisso do artefato	
md5:	cb3410524ec48e9f279e177b7317d4ac
sha1:	7a9ee7131ceb522ce6ee9da968537c472c5ca677
sha256:	b9b19a8f74384601fd0ef8b2f8f4f202ee17c48d25a4e4073ce81b2f3dec8080
File name:	loveyoualotwithfromtheheartotdayloveyousomuch.doc

Tabela 1 – Indicadores de Compromissos de artefatos

Indicadores de IPs e Domínios

Indicadores de IPs	
IP	3[.]145[.]88[.]189, 23[.]94[.]206[.]107, 23[.]94[.]236[.]203, 23[.]94[.]239[.]93 23[.]94[.]239[.]119, 23[.]95[.]60[.]74, 23[.]95[.]122[.]104, 23[.]95[.]235[.]10 23[.]95[.]235[.]35, 23[.]95[.]235[.]86, 45[.]32[.]86[.]119, 45[.]74[.]19[.]84

	45[.]227[.]161[.]55, 46[.]27[.]49[.]180, 50[.]3[.]182[.]140, 66[.]175[.]208[.]79 66[.]228[.]43[.]8, 70[.]34[.]197[.]128, 70[.]34[.]220[.]238, 72[.]14[.]187[.]87 83[.]137[.]157[.]51, 94[.]156[.]65[.]225, 94[.]156[.]69[.]17, 103[.]27[.]132[.]200, 103[.]29[.]3[.]200, 103[.]67[.]162[.]213, 103[.]133[.]104[.]112, 103[.]183[.]114[.]5, 103[.]186[.]65[.]80, 103[.]198[.]26[.]111, 103[.]237[.]87[.]56, 104[.]247[.]204[.]205 107[.]172[.]61[.]136, 107[.]173[.]4[.]5, 107[.]173[.]4[.]15, 107[.]173[.]229[.]146, 107[.]174[.]138[.]160, 107[.]175[.]3[.]22, 107[.]175[.]31[.]187, 107[.]175[.]92[.]68, 107[.]175[.]113[.]202, 107[.]175[.]113[.]204, 107[.]175[.]113[.]216, 141[.]98[.]10[.]56, 147[.]185[.]243[.]107, 149[.]28[.]109[.]84, 149[.]248[.]54[.]207 154[.]38[.]188[.]98, 158[.]220[.]80[.]156, 167[.]86[.]86[.]15, 170[.]75[.]146[.]119 172[.]86[.]76[.]208, 172[.]202[.]120[.]36, 172[.]232[.]8[.]161 172[.]232[.]163[.]207, 172[.]232[.]170[.]236, 172[.]232[.]172[.]53 172[.]232[.]189[.]7, 172[.]233[.]129[.]114, 172[.]233[.]130[.]11 172[.]234[.]249[.]47, 172[.]245[.]163[.]139, 172[.]245[.]185[.]30 172[.]245[.]208[.]3, 172[.]245[.]208[.]19, 172[.]245[.]208[.]28 172[.]245[.]208[.]34, 172[.]245[.]208[.]126, 172[.]245[.]214[.]91 185[.]254[.]37[.]80, 188[.]127[.]231[.]198, 188[.]127[.]249[.]32 192[.]3[.]95[.]131, 192[.]3[.]95[.]135, 192[.]3[.]95[.]216 192[.]3[.]108[.]47, 192[.]3[.]179[.]133, 192[.]3[.]179[.]162 192[.]3[.]241[.]235, 192[.]99[.]190[.]119, 192[.]210[.]214[.]26 193[.]56[.]255[.]218, 198[.]12[.]81[.]138, 198[.]12[.]81[.]158 198[.]12[.]89[.]23, 198[.]12[.]91[.]244, 198[.]23[.]156[.]251 198[.]46[.]173[.]145, 198[.]46[.]174[.]147, 198[.]46[.]176[.]159 198[.]46[.]176[.]175, 198[.]74[.]57[.]54, 207[.]32[.]219[.]82

Tabela 2 – 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**
- **ptsecurity**
- **Bleepingcomputer**

heimdall
security research
A DIVISION OF ISH