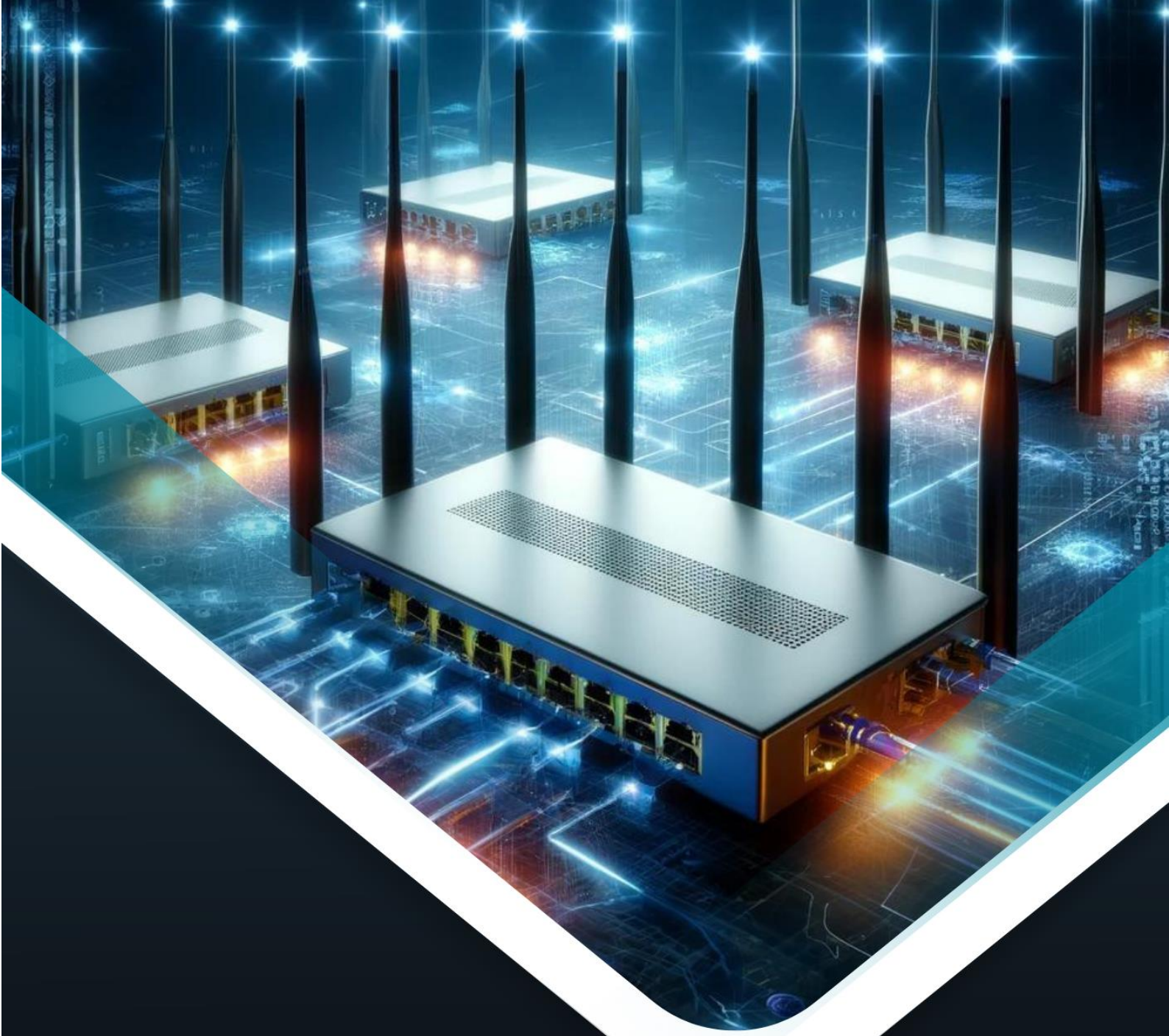


BOLETIM DE SEGURANÇA

Botnets continuam aproveitando falha em roteadores TP-Link para Disseminação Global

heimdall
security research
A DIVISION OF ISH

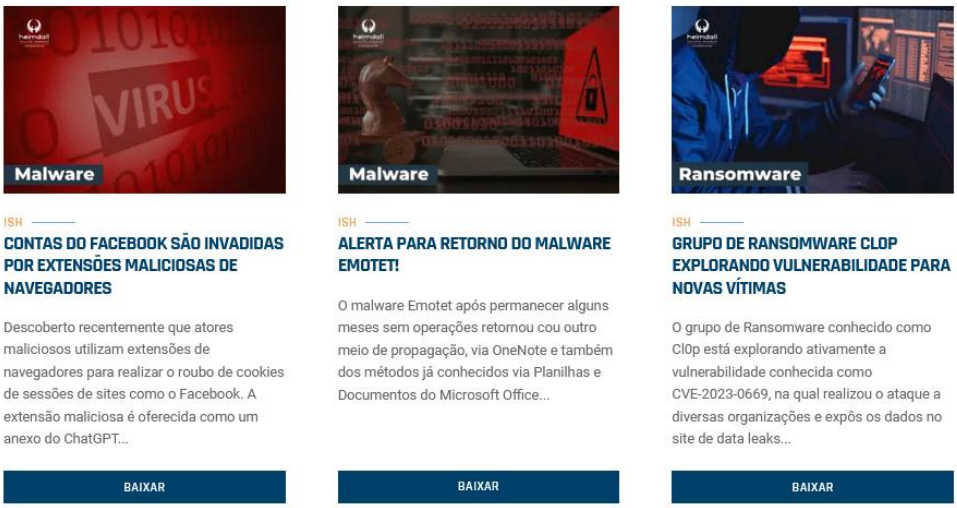
TLP: CLEAR

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 vulnerabilidade CVE-2023-1389, presente na interface de gerenciamento web dos roteadores TP-Link Archer AX21, tem sido explorada por diversas botnets para a propagação em larga escala. Essa falha permite a execução de código remoto por atacantes não autenticados e foi amplamente visada por malwares como o Condi e variantes do Mirai, que visam construir redes de bots para ataques DDoS, alerta a Fortinet.

2 DETALHES DA VULNERABILIDADE E EXPLORAÇÃO

A CVE-2023-1389, é uma vulnerabilidade de injeção de comandos identificada no firmware do roteador TP-Link Archer AX21 (AX1800). As versões do firmware anteriores a 1.1.4 Build 20230219 apresentam essa falha no endpoint /cgi-bin/luci;stok=/locale da interface de gerenciamento web. Especificamente, o parâmetro "country" da operação de escrita não era higienizado antes de ser usado em uma chamada para o popen(). Isso permite que um invasor não autenticado injete comandos que serão executados com privilégios de root por meio de uma simples requisição POST.

```
POST /cgi-bin/luci/;stok=/locale?form=country HTTP/1.1
HOST: <Vulnerable Website>
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: <User-Agent>
Content-Length: <Length>

operation=write&country=$(<Malicious Command>)
```

Figura 1 – PoC da vulnerabilidade.

A Fortinet detectou várias explorações focadas nesta vulnerabilidade, com destaques das botnets identificadas estão, Moobot, Miori, o agente “AGoent” baseado em Golang, variante Gafgyt, e outras que foram adaptadas para explorar essa e outras vulnerabilidades. Abaixo é possível observar o mapeamento destas explorações.

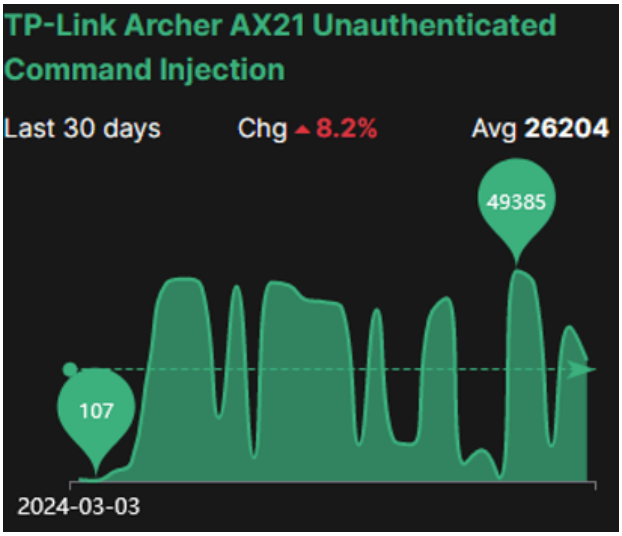


Figura 2 – Telemetria de IPS-1.

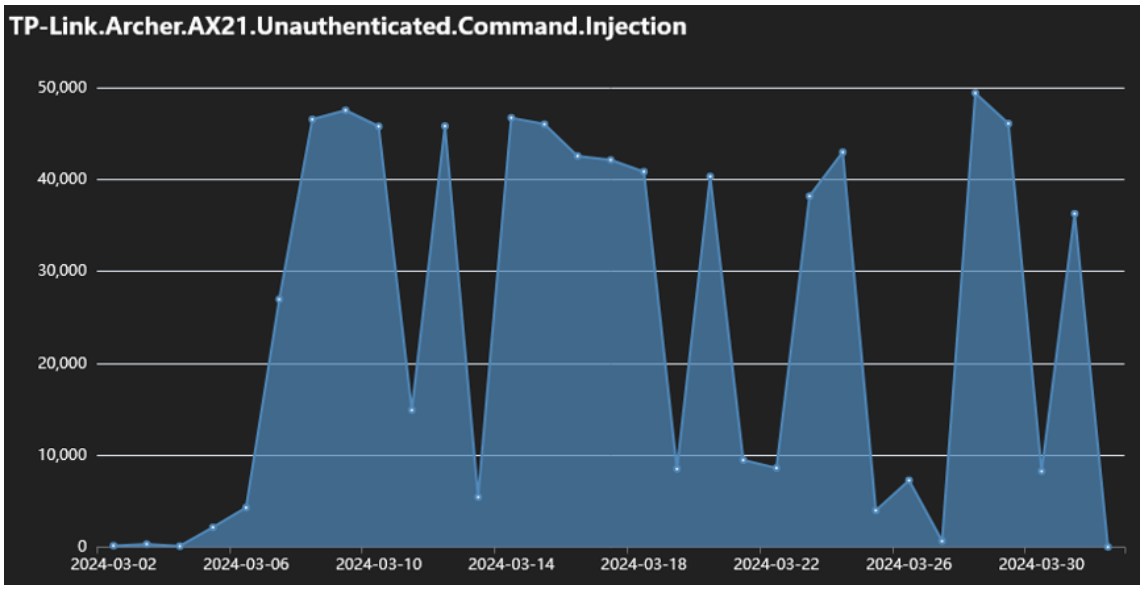


Figura 3 – Telemetria de IPS-2.

3 CONCLUSÃO

O contínuo abuso dessa vulnerabilidade, apesar de correções disponíveis, destaca a importância de aplicar atualizações de segurança prontamente. A falha expõe as redes a interrupções potencialmente devastadoras e comprometimento de dados, enfatizando a necessidade de vigilância constante e adoção de práticas robustas de segurança cibernética.

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:

Atualização e patches

- Garanta que todos os dispositivos afetados, especialmente os roteadores TP-Link Archer AX21, estejam atualizados com a versão mais recente do firmware que corrige a CVE-2023-1389. Verifique regularmente por atualizações de segurança disponibilizadas pelo fabricante.

Segurança na configuração de dispositivos

- Altere senhas padrão e desabilite serviços não necessários. Configure firewalls e sistemas de detecção/prevenção de intrusão para bloquear tráfego suspeito e monitorar atividades anormais.

Segmentação de rede

- Divida a rede em segmentos para limitar o tráfego entre os dispositivos IoT e outros segmentos da rede. Isso ajuda a conter qualquer infecção que possa ocorrer.

Monitoramento e resposta a incidentes

- Implemente soluções de monitoramento de rede para detectar comportamentos anômalos típicos de botnets. Tenha um plano de resposta a incidentes para agir rapidamente em caso de detecção de uma infecção.

Educação em segurança cibernética

- Treine os usuários e funcionários sobre os riscos de segurança associados a IoT e ensine práticas recomendadas de segurança, como a importância de atualizações regulares e vigilância contra e-mails suspeitos ou links maliciosos.

Backup e recuperação

- Mantenha backups regulares de configurações importantes e dados críticos. Isso permite uma rápida recuperação em caso de um ataque bem-sucedido que comprometa seus dispositivos.

Uso de ferramentas de segurança avançadas

- Utilize ferramentas avançadas de segurança que incluam capacidades de sandboxing e análise comportamental para detectar e bloquear tentativas de exploração antes que elas causem danos.

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:	28780ceae317b5d0388ad6a68baf4dc8
sha1:	0eaa8aa94bde69edb13aad4aa9cd9ebeeb6a29f2
sha256:	6104674bfa58ac11c697062d6068c568384f13037d1a146dbe25cd001104ca8b
File name:	bot.arm

Indicadores de compromisso do artefato	
md5:	36ae69640d3fbaeb88943933ec3a31a2
sha1:	bfda0689bc72991b6e314b89663f7d1595cd2755
sha256:	f33a02781d60ca36f4ee56579c6d33846c2549ad7556bca499c73302cee17514
File name:	bot.arm5

Indicadores de compromisso do artefato	
md5:	1cd4eb4c77dc51866510868f63c9c289
sha1:	9704ed49a81cb5c600cfb5a21266a7b4cea59bd4
sha256:	d02381634921d92358577c106180eba766b98a520c907870898b2c32d7de4547
File name:	bot.arm6

Indicadores de compromisso do artefato	
md5:	bf604b730f06057768b6f4ae8b7a7ba1
sha1:	eb542707ddd3212ddc34cb90829edfc5b5e51a48
sha256:	0a3fbc79e742354c8fc82830fc3426f7f8d3b900260c06aa58e53547b48feaa6
File name:	bot.arm7

Indicadores de compromisso do artefato	
md5:	7e29353af3efc6a749806c3c5c5ca7d2
sha1:	36f0a20cf3f1526535bd6eb578ea01cf845a7da9
sha256:	475487bf7b96fe3da321dac0b5f59231651fc3d71f86bf9580bfa77e59b0f2c8
File name:	bot.m68k

Indicadores de compromisso do artefato	
md5:	6189da58eb6ed748f69836dac6233d21
sha1:	bbf11ae938371c602a12036e840a06925eb15430
sha256:	a3e8493f2fb38b7f2ba309809577281d3cc25bee9fb3b5c0053a6e89de1dbce7
File name:	bot.mips

Indicadores de compromisso do artefato	
md5:	81374da09faff8bad8ab7b009dedf4f7

sha1:	f247f077f9dc8caa17de29ed14cf4e4f6d635f6f
sha256:	5e6deba076cbe7b9833d0ddee7c8065e91d13f1fc2a5c7daf4db36da458d689a
File name:	bot.mpsl

Indicadores de compromisso do artefato	
md5:	7475fb2adf7f559a6e4ce4666286df19
sha1:	5ef7b9b101ad23c02cd37268fbf351616fc7e698
sha256:	29ef4c5d9172b09d6abc08da800a5a09b460b98aaadf1aa29edda81300fcc609
File name:	bot.ppc

Indicadores de compromisso do artefato	
md5:	cdba14dc7070bfe3f5fe953d81684f83
sha1:	5dfeaeb9d4a88c8c06d03f13025c2c0fd00645f2
sha256:	e7af5f1d5d68f75ee03a37ee8016695e35edaae528cdba4ab7b9a90570a1e4be
File name:	bot.sh4

Indicadores de compromisso do artefato	
md5:	5a5bfc214e1fa24d4507d147977de82a
sha1:	ab2ffe6c2050e20aa400565e4816186a6fd5ac3a
sha256:	b45906c711ed4f109a10cfaffa0b4c18e56c6f6ddc8d100c87e0a0349a30293d
File name:	bot.x86

Indicadores de compromisso do artefato	
md5:	32bb9394becff61da26cc51cbdcbfcd0
sha1:	aa10646adcd70d1abc181323b26eb5d77aa169e8
sha256:	e9e8fc16c586f51eb2f86db5a60e54b46d66275fdd6df8fb72e96e50014a1290
File name:	bot.x86_64

Indicadores de compromisso do artefato	
md5:	e1bf81513c4978da8bff910032ba905e
sha1:	e35b9437874c6c71a5894914cb6bb211a94f6038
sha256:	1ffc3c457eb84aa36cd4bc7f3d0dc9a6b8079d63c2bab03c3a646906152876c0
File name:	arc

Indicadores de compromisso do artefato	
md5:	bc2fb94ed641b2659644a4a763a273ac
sha1:	8f9a7fdf8782c8b974c9456a8a57a7f0143a79a9
sha256:	d8b4d8950ec1a3f812af69d261f452aae2b19d3bced8551f9178e40ca0c1bcf8
File name:	arm

Indicadores de compromisso do artefato	
md5:	03afd9f73e4aea49e39330f5a164445b
sha1:	799e623d0ae128ead5127af02f86d8e3d082c1b6
sha256:	8562c9ad26ab3ad7d16ac43c9dcbf600d5319e5432d72dc684983cc5f64ff41e
File name:	arm5

Indicadores de compromisso do artefato	
md5:	e9eaf49d263f78eb80b035dd1224057a
sha1:	be9436f868387a0f67c1fd657dea7460eb38c717
sha256:	092b3a57ee4ecd64591616da6ce0cfb9f01930dbeb179f05e1dbbdbc918098ac
File name:	arm6

Indicadores de compromisso do artefato	
md5:	d3f2541625596ad1e14d475c5ab52bf2
sha1:	84bbccc973efd723eebd93c01eb9a996011c0001
sha256:	c65f86d5917025a8674bf9758870decd923ea2662d6611a1365303f4fe55fa26
File name:	mips

Indicadores de compromisso do artefato	
md5:	34518c5a21f0daf44657ba7b4024cedd
sha1:	b68134eb6c77426bea9121c2a27cf0eb01e2637b
sha256:	65f64b270a10255db1e55a158a02829a3af982cbcd4b56f14e58132cbb45e6a9
File name:	mpsl

Indicadores de compromisso do artefato	
md5:	29a40fc2e5bcd633cb42d1b05cb675ee
sha1:	c7f2681207baa7f61ee64191e648c2ba3da0b9af
sha256:	a383319a28d50e8c280646dc53a2f33fec62ad69ef4948dae76a4f1f6fe2f159
File name:	ppc

Indicadores de compromisso do artefato	
md5:	a07661cb4f796eabeb714a1cc91f4b58
sha1:	11eb3294a067c8489dda2cc91db973f7af8c9dea
sha256:	7ef190f05fe9be5d7f38bdb556fffdb7d9b5633ddf60cc43b98c09887a292c49
File name:	sh4

Indicadores de compromisso do artefato	
md5:	1e1c7a41e949214c642944bc82b6ab2b
sha1:	0a26baa4767477b52887ef26e8b7a4d6a04fcd57
sha256:	7322da39ce05e7496fcaef6602a15266943a59a5027e5ea97344133d42e0f6e3
File name:	shk

Indicadores de compromisso do artefato	
md5:	dd80ff5207f33b03479354ddc1169099
sha1:	a369453c8a93c8d0fae1c0e0ee2d7d763902f2b6
sha256:	a1c14e99cc8490a4d503ffd660e2d881fa5d766a4288eea328f73bd8ee99078d
File name:	pending-libc.txt

Indicadores de compromisso do artefato	
md5:	54cf833da2312e55e248de6474230444
sha1:	01ac751b72516449460b2fbcceee02dd510288c3
sha256:	a7d3ffbb3edff1956d7422dd04305d8c3ac16418e2eb190ed9a08a1c275c5e8e

File name:	arm

Indicadores de compromisso do artefato	
md5:	b351d50c60b74645130922ea89356c75
sha1:	5f9780fb28d86e243ee8fb294e2930da9ca0b8d6
sha256:	1427deedaafd5345aa3c41d39b14b23a454ed894c73f3c9224cd0b51c88afcfa
File name:	arm5

Indicadores de compromisso do artefato	
md5:	a7d8d8313ee507ee28f5a1775026b2a0
sha1:	a6219e8c30e6233c8c483646e3a34b64cd2a2644
sha256:	f97c9802324eeb0ebdfc15ce3e390c8cca5a9062c3348f7d2b5b00d1efa49508
File name:	nigger

Indicadores de compromisso do artefato	
md5:	50f622cba193eeb1bde097fbe120e045
sha1:	05d0062cd6b6d38e3f2bc73ed12e5cd17e412b80
sha256:	3307e4d1daefca1eeb1ee4a6dea7738594076aa04f3e7e470a8b2ae32b9e4893
File name:	arm7

Indicadores de compromisso do artefato	
md5:	94ea9d6040f2ac7b62111b9ce88d7d0f
sha1:	67f9d2bc005c6ba9c9b13f1aeac0d09da29c3713
sha256:	86fe87891311228b58a606114a2d41d94b520c5c4be6ff6bc0add45f5b6250ef
File name:	nigga

Indicadores de compromisso do artefato	
md5:	c3127080466a78826d8580f8a566a025
sha1:	1abced23eda7d0107e18b3dba45eb282fffc6354
sha256:	b9962c3e066904cf8df05f60b9bd21d979466aca64596d2b7557be7fa4358c4d
File name:	kekw

Indicadores de compromisso do artefato	
md5:	497399ad8afc83012558fa6459431004
sha1:	3ab230143b3270134ea4b569b8a18cb1878453d4
sha256:	a48807aaa7be63c41bbabcf55d40cba416bc23432f247e4038ed0cd32fd05519
File name:	shiteater

Indicadores de compromisso do artefato	
md5:	ee6fcd7ef99edbac2d35ab6338da40c4
sha1:	b3b06b59c7cb54ecd60362b037a460333e3588b3
sha256:	4119530c4dba8a53ba081094ca163f28a51bd37c6ee40b4aa55097939ec1df38
File name:	mips

Indicadores de compromisso do artefato

md5:	841182fcdf9965544cbcc51ce331110e
sha1:	b52eb57fc6e3f2d0475ef31eb5b3db1c8daabaee
sha256:	2be7481bfec8fcbb370afa00e9befa97000e7aa987a17cd6c48fc9f2d0b60110
File name:	lmao

Indicadores de compromisso do artefato	
md5:	df8274a6ba57eb663e46b5a82384b09c
sha1:	0ffc8e8e8c0d98a0fad7802300d92cff09a0be13
sha256:	b605570db3158ba355552b5b638e7df4b0888d56d206004d9af6901c4770c75f
File name:	what

Indicadores de compromisso do artefato	
md5:	02e3ee0452d7ba33a9bb15310a7271a9
sha1:	a25edffd5c592b83917767ec9a141d9f2ff67bd0
sha256:	0dbf4c327df0159305ffc9776ad2fbdd655fe513712f75e360e211aa6686f69a
File name:	11498

Indicadores de compromisso do artefato	
md5:	329545a5748ae518f469f8f19396becc
sha1:	7a574bfbee619267e5818f5484c82c24d7e9a516
sha256:	ae2d6b41150d61b828368847a0eba51d4562fa2bae4478c10940f5e3e3e46c6b
File name:	blyat

Indicadores de compromisso do artefato	
md5:	e77b911a34bde296048c09f1e444a6f8
sha1:	5aed61d234e32ba637007ff12b8645a686e858d7
sha256:	18753e0c31c2100889f0e085ba03eb1c616dcc50606d9733574b68e75be2ee7a
File name:	x86_64

Indicadores de compromisso do artefato	
md5:	9ce767ed9ced78fe8f35fef70c1d93f4
sha1:	c2ed785ca62cf88038eef7f287542763d061dfcb
sha256:	123a392cfa9114daeab28976f5ce740da4288d6ac516b5afbf1ea17e28eaada1
File name:	1.sh

Indicadores de compromisso do artefato	
md5:	1ccc9347f5aaf93e87f894edfaf90766
sha1:	d68e9153ff13ab93711b0a82c58f23d2cbf5ca31
sha256:	8317c084d08450a220fe7f38ce6b1a767b2e8776f8f4a436b84b912476b00cbc
File name:	5551

Indicadores de compromisso do artefato	
md5:	1779ed9f14f9eed7fce73b1c0260973d
sha1:	f4f8778c0c493654f622ccc2c32efd356c5702ce
sha256:	94c9297951a48fcc0f22dac94da599bc2651c757d27cb94c9de16d00ea5af04f
File name:	9813

Indicadores de compromisso do artefato	
md5:	9c787a93b22e30383ecfc7f1f28b6b36
sha1:	13779e7053ba689fbe5902caecb14816f9b93f59
sha256:	fdcfaa03f99233d8aecc17098833d82860d68c12440c5ff7e898b50891cf65bf
File name:	arm5

Indicadores de compromisso do artefato	
md5:	d0f756b78b0cf9eb7b575c8b4e355ec2
sha1:	abccef2b932e5737fb0b9b3a6905d63dd141d363
sha256:	045b8b9f7bb69e4450d49eb6197722b9b58a8f0e7af479640ea6f666553db4da
File name:	arm7

Indicadores de compromisso do artefato	
md5:	f817992ebd08cf11a64ff81a3900b933
sha1:	b6353f5135469a4c5ef03515479c62067aaca3c1
sha256:	96c8ec9a54b0fef4bca739b47d943c295c766c7759d0f3a5a891585609019f42
File name:	i586

Indicadores de compromisso do artefato	
md5:	de711aef83f7baa89004e1fc3aaee4b5
sha1:	cd9cda7b7fff8cbb46ec032c7fd0452c93afab69
sha256:	1a6964f76f573dd50f41ee8dc4c5b29868807af6326faee92ad9ffaeba3dc5a3
File name:	i686

Indicadores de compromisso do artefato	
md5:	2897bd787249aca8860f70c228792a6d
sha1:	6fee89bfb2cec44cb46a9303dcb11e1a1c4f3969
sha256:	e220a88f3c07a6ece0adcbeca93fd6024d9f63a971c4aa732ec90930e386b5aa
File name:	mips

Indicadores de compromisso do artefato	
md5:	ca46e62190726aa4f1692cf4e1244d04
sha1:	60d5e4c2672184c3aee0d2c1483e0549505b607d
sha256:	42deb408f0861891e49205fce2496cfe9a6c0cbf86f5d1c48bd88f9120631b1d
File name:	mipsel

Indicadores de compromisso do artefato	
md5:	daa990374ae49857dd9c3e4569cb4710
sha1:	0d582250b7bc5971654da167e84009acfaffe1c6
sha256:	f19d69486f380f7f22482b17eab7343da36229a4e60b9f3938f7846002ff0fa2
File name:	19084

Indicadores de compromisso do artefato	
md5:	6800ddae74cc2547cc30f3144cfd8bc5

sha1:	b32218411fb04b44add99d30a65769ac2ad82938
sha256:	8721dc3617731683a34eb7c8d9a688195d2db1efa8da3084edbe04f76cb0d047
File name:	sparc

Indicadores de compromisso do artefato	
md5:	0e14b39261e45febc077c1f46801df77
sha1:	383c227aaddd24d98915edf0dc5e4e60ffe023fa
sha256:	7e8061fab5ad856312040a78674932dcd08b6926a8cc8a5de91252c590b4f6ba
File name:	x86_64

Indicadores de compromisso do artefato	
md5:	9e0d1124dae07a104dcb93b2e27e8ddc
sha1:	c310ec9924e2371402e8d3df66624a126a673996
sha256:	9100bc0eb0bce4f5f7fc314fa820b4dee00db8d31892ec6fdb4fccca801a40d0
File name:	9100bc0eb0bce4f5f7fc314fa820b4dee00db8d31892ec6fdb4fccca801a40d0.elf

Indicadores de compromisso do artefato	
md5:	edde29aa21d33640bce8a63c5dab3e07
sha1:	c5a51c32cea976982747e19c90da8a3fc73b5e3d
sha256:	46d085e7c36ec4ada5f630c47b1ed418ceae077832d6fc2e7730af2715fb954d
File name:	46d085e7c36ec4ada5f630c47b1ed418ceae077832d6fc2e7730af2715fb954d.elf

Indicadores de compromisso do artefato	
md5:	1fe9cdb00a4cc5b818d4c956a7764b18
sha1:	617af7c8a51e87da152b2dc4b5459f7d424c5289
sha256:	cc197f92fb6564575d7bd64958bc96be9e0c09d06fa19449a0ad3dc50f09ddb6
File name:	cc197f92fb6564575d7bd64958bc96be9e0c09d06fa19449a0ad3dc50f09ddb6.elf

Indicadores de compromisso do artefato	
md5:	ff5d1c56dbf02732678f509fbdfc4f62
sha1:	5e25e5ee87a83785a9d881aceec2f4b13768021d
sha256:	4e94d9808d5c3c414100abb60233614fcbad2e884c2fd851cb9d694186165a4f
File name:	4e94d9808d5c3c414100abb60233614fcbad2e884c2fd851cb9d694186165a4f.elf

Indicadores de compromisso do artefato	
md5:	4eeac4436b9c68f85b1c3a2bae62d3f3
sha1:	4895bfd63ba3ae5fd97f69c4a243d4bae7eddfa1
sha256:	bfa195bd238473bfead86e74b796c4721d1f5281c284b96ff29d8806a82a6520
File name:	exec.sh

Indicadores de compromisso do artefato	
md5:	49aaf9125d326aa623fc037b50811ace
sha1:	147988acf0712988e3cc63232fe8cc70a0dea5f9

sha256:	396b1e21260b374a45ba703239bc29b1345dea89ad9d54db0b7f312aa95c6984
File name:	396b1e21260b374a45ba703239bc29b1345dea89ad9d54db0b7f312aa95c6984.elf

Indicadores de compromisso do artefato	
md5:	1198f93e9223bc9638414da7a4c31b4f
sha1:	c57bc8673681c305f4c53bce09a9f7deacc69bb1
sha256:	1a1a8f9ccb66f37f14b5cf2a77e9e8d47400bdec957d9f20729e5c81bfc78be6
File name:	1a1a8f9ccb66f37f14b5cf2a77e9e8d47400bdec957d9f20729e5c81bfc78be6.elf

Indicadores de compromisso do artefato	
md5:	22a8bf2952fb7d02badcf3d52f40181a
sha1:	ad8672625370a13b270abd2e0a7f51ce4b1cdfb2
sha256:	699d00adf4e8c070d2b955b23054e945c78267beb2ec9cc580130771200e5ea3
File name:	699d00adf4e8c070d2b955b23054e945c78267beb2ec9cc580130771200e5ea3.elf

Indicadores de compromisso do artefato	
md5:	91617304b71d42f0afa0e5eed013c5c9
sha1:	2361f28f6785d70b2e01616768c6a9e7a717fb97
sha256:	fdae7846f75c7b65130e73bafda28f442913e403534cb91657c21c2426869f2f
File name:	mipsle

Indicadores de compromisso do artefato	
md5:	997b1a8905e9277bc2b4b0691c16d5ac
sha1:	cc3ff6898266c8ed09d66bbae805772ef066036f
sha256:	25f3558a2cdf5aca294254004954bb10d08a0ef0f913f3ddd1f8f3cc71f114dd
File name:	25f3558a2cdf5aca294254004954bb10d08a0ef0f913f3ddd1f8f3cc71f114dd.elf

Indicadores de compromisso do artefato	
md5:	50ba3e664b50e73d29623772c2428a4b
sha1:	dcbae4a9375de727d8cc6d53ecd4cd7f39a831db
sha256:	12273047ec3eb4e1318c26ec7c10b77e5d631738da126880e248d7f54dfa5718
File name:	12273047ec3eb4e1318c26ec7c10b77e5d631738da126880e248d7f54dfa5718.elf

Indicadores de compromisso do artefato	
md5:	8d2d00cb140637a40cf5c16998a009d2
sha1:	07595f552498d9dc6d6b467223557e2e7c806e31
sha256:	f7faaadceebe69bec33096166a54ed9b593b1b690ba9594b4c353303f55101aa
File name:	s390x

Indicadores de compromisso do artefato	
md5:	10ee40812ca3f89f9aab076f5ed9d677
sha1:	4f6a86749cb95ee96911b0c6443ae0a1bafb9aca

sha256:	e6d1df0621b10d051ebba4507ac3d14f4d206ab56bafbc3510db542d4c4470d9
File name:	bins.sh

Indicadores de compromisso do artefato	
md5:	f8855bf7a1b2240918bd21d05a9ef789
sha1:	700d3c35db19ba525f1076fc35e8937df756911b
sha256:	4480d72a324f519d3a630bf2ef7b118f4e388c5bccdd0a5465bafd2253daa619
File name:	rebirth.arm4

Indicadores de compromisso do artefato	
md5:	9276946341d81db5eeabc777caacb99d
sha1:	7c56380e28df0eee301ae3608043cbac8a74af1e
sha256:	4509e84a9abcb732f0ee90bf27dd300247b23b6dac9b41cd01f59d6384b5348a
File name:	rebirth.arm4t

Indicadores de compromisso do artefato	
md5:	47ba70b30895d949cd78ee34a97b779c
sha1:	25820a7de1a1052a9ea4779679e4050d96979a55
sha256:	08166a0d2fe65a3ad8b289cb2714c3a150635e29664bff24e5befc6b48526899
File name:	rebirth.arm5

Indicadores de compromisso do artefato	
md5:	918ddc07f27b1ceec21cdc0e90e3a802
sha1:	306b48c7bc12ab987ee9f9fcd5a2aae7cfb6ac00
sha256:	ed85c3e25bac63b7e232ac3cfd91116bf7c64f1c4c96b933d5715bbe055ffc89
File name:	rebirth.arm6

Indicadores de compromisso do artefato	
md5:	6afb6ce3b5eaac5a043b3c10a906deff
sha1:	824cec63144c6b878f1716142001cfffc5bbaaf8
sha256:	f0d62aec4a2a5353a6416bbd403969fc0617d08aeb8eb9e09de4d4068a2fd9f3
File name:	rebirth.arm7

Indicadores de compromisso do artefato	
md5:	7b5d70f2ae145d3ffd0aece973ea3314
sha1:	2f1081711952ec0aaf93d886bc5636d96da756d4
sha256:	8cfdcaf4611fd855672ad561de196417deea97341f45efd02e97e26d4674291d
File name:	rebirth.i686

Indicadores de compromisso do artefato	
md5:	36a6d7af6b8c1502a5cd77178b29473c
sha1:	80c555971244e4834714628b681c0ab9b7248184
sha256:	e73bbef9c7fcaf610c858be52a375b517bc62fd7e05dd867f928cd353536de16
File name:	rebirth.m68

Indicadores de compromisso do artefato	
md5:	ce638753065f91224f07020a456cbe9c
sha1:	912671cbe26bd6b7d1fee23e3f9d208d1beb1108
sha256:	c192146c8311694342f73a19cfe69ecc53f3f1d6cab006526d2daa5134846357
File name:	rebirth.mips

Indicadores de compromisso do artefato	
md5:	9e7502a085f10b02c1fa8c82df796f9c
sha1:	4aaa7e9d5860c7be2b364cf9b12d691aef8c6f4a
sha256:	ab5ee18fd3df5a2d7f2d84c75b33fd2f73b76c8e0d2df278d9ded40943d16911
File name:	rebirth.mpsl

Indicadores de compromisso do artefato	
md5:	f2c2ec92b3c64199555b761fedf79c4c
sha1:	6de4684a34e14d83c1a74b3617bbf27c50e708ba
sha256:	ef30bd34f8c11e042e2600c62cf702515c94290207cf72fad1ec0d277221bb70
File name:	rebirth.ppc

Indicadores de compromisso do artefato	
md5:	afa66c3c8751f268dce635711f5895be
sha1:	259e21ff16beef255c751bc64c0fdbbfdd67f0ff
sha256:	0571c16d0f2d0267b354f81fdbfb49738f3cb867371b9ef0d3ffe1020fb9f9cf
File name:	rebirth.sh4

Indicadores de compromisso do artefato	
md5:	b593ee2d3a9fdf1621295fd0d7a7cf53
sha1:	bb89765d73e4f702c8df9b352ad4e7146c456868
sha256:	bf5e6947f6829d17b8a8e5984366efcf5592d8f6bc7ec6d7e85b1872bebcb24a
File name:	rebirth.spc

Indicadores de compromisso do artefato	
md5:	11932ffe67998c0b9226a0ec35b059ff
sha1:	42e1048b5682bf20af13a5e535967b29da426b69
sha256:	549d3aac3b42f702f29ab27c653c0f239a51601a6aeb50564beda614f8f1f33e
File name:	rebirth.x86

Tabela 1 – Indicadores de Compromissos de artefatos

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
URL	hxxp://91[.]92[.]253[.]70 hxxp://94[.]156[.]8[.]244 hxxp://103[.]188[.]244[.]189 hxxp://185[.]224[.]128[.]34 hxxp://5[.]10[.]249[.]153 hxxp://195[.]62[.]32[.]227
Domínio	rooty[.]cc

	bn[.]networkbn[.]click fjsnsinfinsf[.]ngcv[.]top
IP	45[.]155[.]91[.]135 5[.]10[.]249[.]153 195[.]62[.]32[.]227

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**
- **Fortinet**

heimdall
security research
A DIVISION OF ISH