

**TLP: CLEAR**



# **BOLETIM DE SEGURANÇA**

**Campanha de Phishing do HubSpot afeta 20.000 contas  
do Microsoft Azure**

Acesse a nossa nova comunidade através do  
WhatsApp!

## 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 ClOp 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	Detalhes sobre a ameaça .....	5
2	MITRE ATT&CK - TTPs .....	9
3	Recomendações .....	10
4	Indicadores de Comprometimento (IoC) .....	11
5	Referências .....	12
6	Autores.....	12

## LISTA DE TABELAS

Tabela 1 – Tabela MITRE ATT&CK. ....	9
Tabela 2 – Indicadores de Comprometimento de Rede. ....	11

## LISTA DE FIGURAS

Figura 1 – Fluxo da operação de phishing. ....	5
Figura 2 – Primeiro acesso SSO do ASN nos detalhes de alerta da organização. ....	6
<i>Figura 3 – Página inicial maliciosa do Microsoft Outlook Web App. ....</i>	<i>7</i>
<i>Figura 4 – Diagrama de análise de infraestrutura do agente da ameaça. ....</i>	<i>7</i>
<i>Figura 5 – Adição de método suspeito aos detalhes de alerta da conta do Azure. ....</i>	<i>8</i>

## 1 DETALHES SOBRE A AMEAÇA

Pesquisadores descobriram uma campanha de phishing que teve como alvo empresas na Alemanha e no Reino Unido. O objetivo era roubar credenciais e controlar a infraestrutura de nuvem Microsoft Azure das vítimas. O pico das tentativas ocorreu em junho de 2024, utilizando formulários falsos criados com o HubSpot Free Form Builder. Aproximadamente 20.000 usuários em várias empresas europeias foram afetados.

A investigação conduzida pelas equipes de segurança concluiu que a HubSpot não foi comprometida durante a campanha de phishing. Além disso, os links do Free Form Builder não foram enviados às vítimas por meio da infraestrutura da HubSpot.

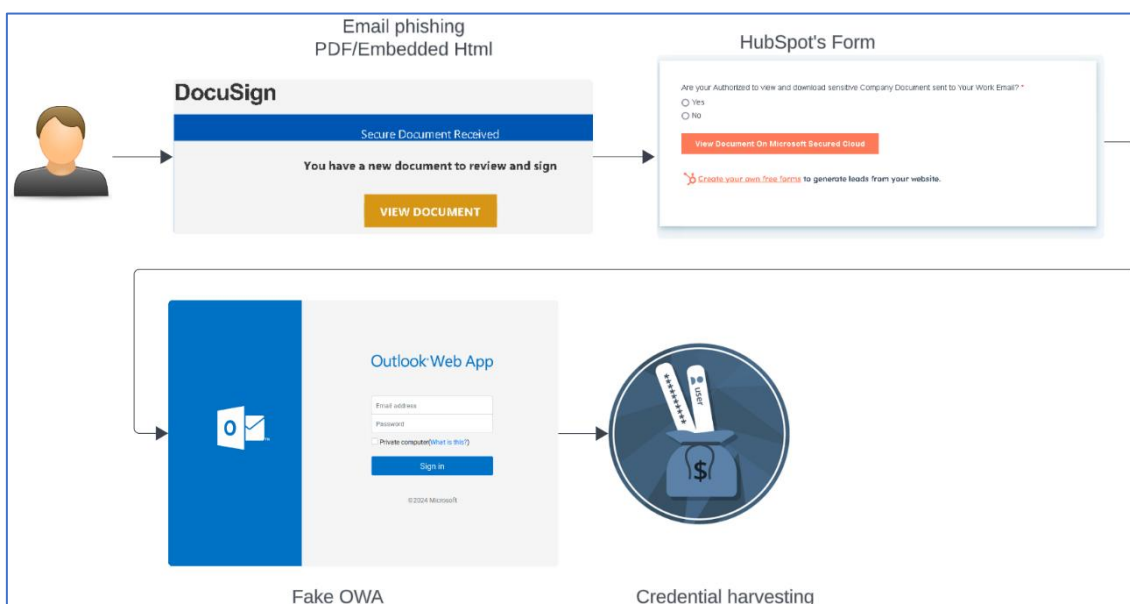


Figura 1 – Fluxo da operação de phishing.

Apesar da configuração de phishing ser diferente, os invasores reutilizaram a mesma infraestrutura. Ao analisar os e-mails de phishing, foram identificados dois indicadores úteis para reconhecer ataques semelhantes: um tom de urgência e falhas nas verificações de autenticação.

Os e-mails de phishing frequentemente criam um senso de urgência com frases como “ação imediata necessária” para pressionar respostas rápidas.

Falhas nas verificações de autenticação:

- **SPF (Sender Policy Framework):** Um resultado “Reprovado” indica que o IP do remetente não está autorizado a enviar e-mails em nome do domínio, sugerindo falsificação.

- **DKIM (DomainKeys Identified Mail):** Um resultado “Falha” significa que a assinatura digital do e-mail não foi verificada, indicando possível alteração ou falsificação.
- **DMARC (Autenticação, Relatório e Conformidade de Mensagens Baseadas em Domínio):** Um “Erro Temporário” aponta para problemas de curto prazo com alinhamento de domínio, geralmente devido a atrasos no servidor ou DNS, enfraquecendo a autenticação de domínio.

O DMARC depende de verificações bem-sucedidas de SPF e DKIM para confirmar a legitimidade do domínio, oferecendo proteção contra falsificação e phishing.

Também foi detectado o uso de um novo Autonomous System Number (ASN) que não havia sido observado em atividades anteriores do usuário, aumentando assim o nível de suspeita. A figura abaixo ilustra outro exemplo de um evento de alerta que pode informar as equipes de segurança sobre tentativas de login maliciosas.

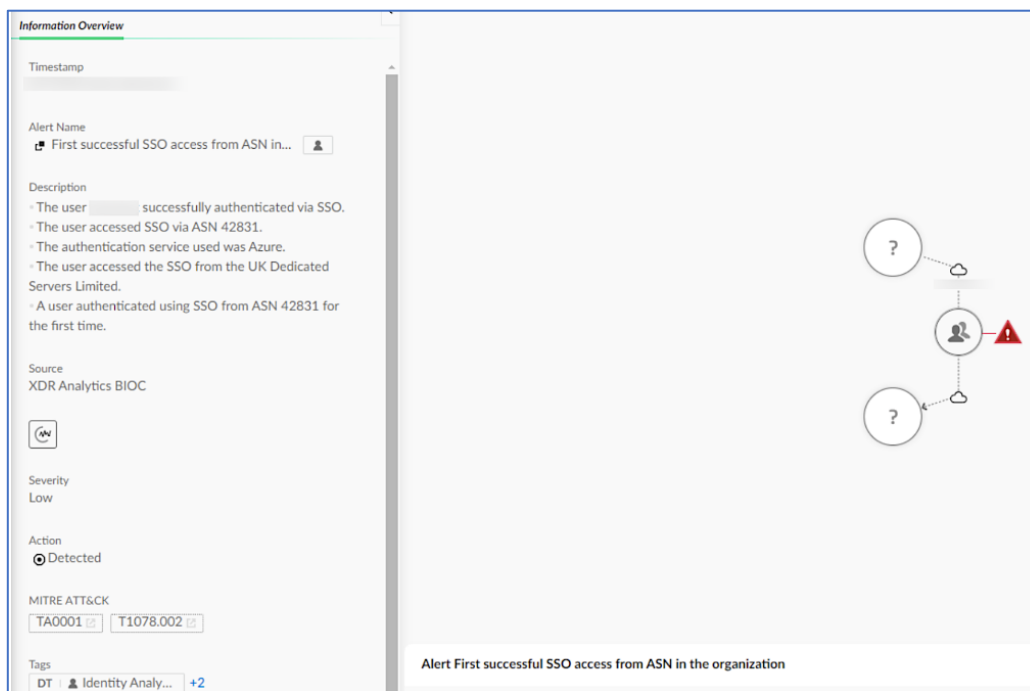


Figura 2 – Primeiro acesso SSO do ASN nos detalhes de alerta da organização.



A análise revelou a existência de pelo menos 17 Free Forms ativos, utilizados para redirecionar vítimas a diversos domínios controlados por agentes maliciosos. A maioria desses domínios estava hospedada no TLD .buzz. Cada Free Form identificado apresentava um design de página de destino e um padrão de redirecionamento similar ao do Microsoft Outlook Web App.

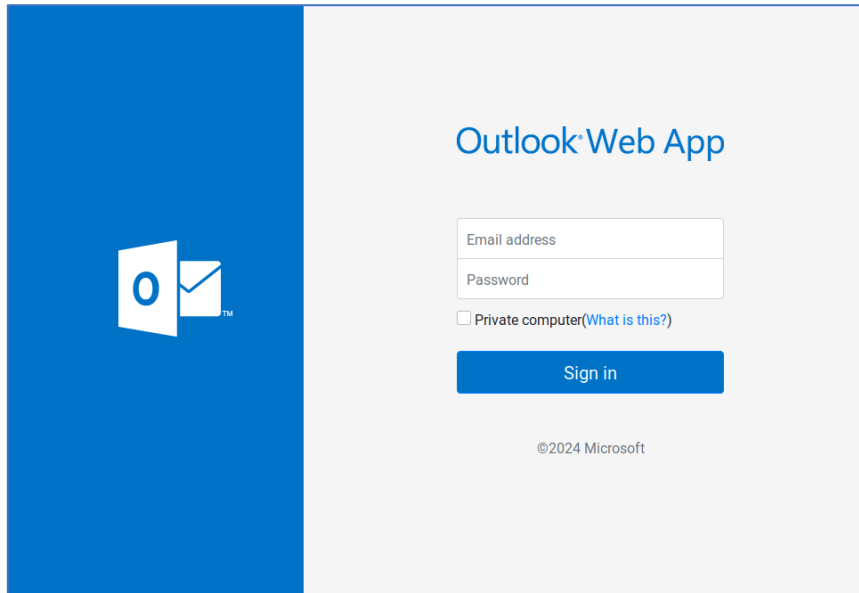


Figura 3 – Página inicial maliciosa do Microsoft Outlook Web App.

A campanha de phishing utilizou diversos serviços de hospedagem, incluindo o Bulletproof VPS, conhecido por seu alto nível de anonimato e pouca aplicação de regulamentações legais, tornando-o resistente a ser desligado. Esse tipo de serviço é frequentemente associado a atividades maliciosas. Durante a análise, foi descoberto que a mesma infraestrutura de hospedagem foi usada em várias operações de phishing direcionadas e para acessar locatários comprometidos do Microsoft Azure.

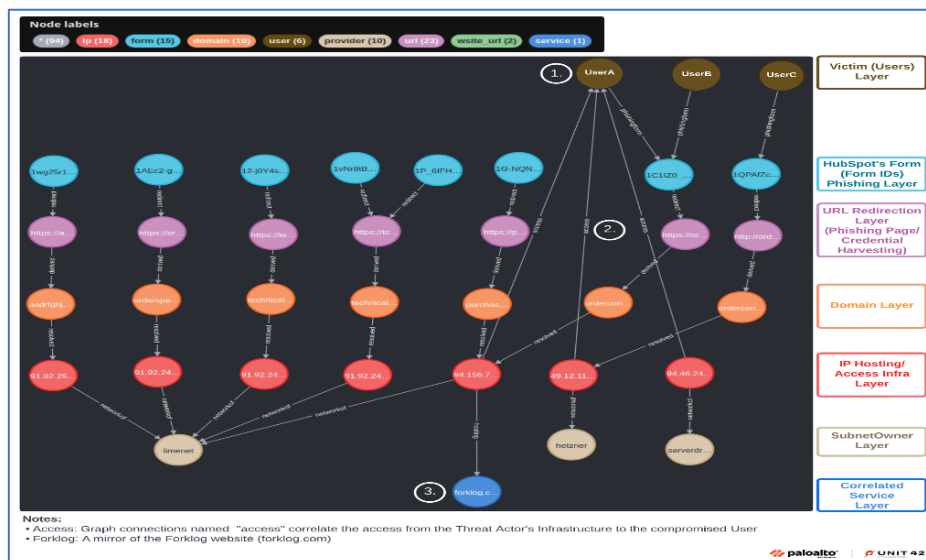
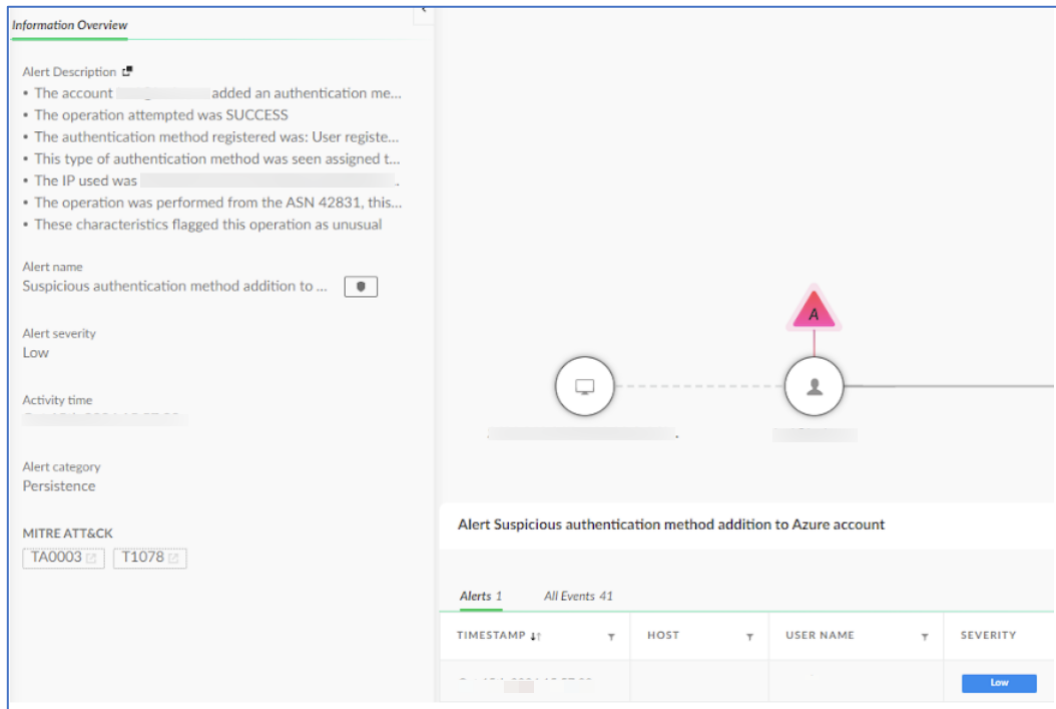


Figura 4 – Diagrama de análise de infraestrutura do agente da ameaça.

Durante o ataque, o invasor adicionou um novo dispositivo à conta da vítima, garantindo acesso contínuo, mesmo após tentativas de bloqueio.



The screenshot displays a security alert interface. On the left, the 'Information Overview' panel contains the following details:

- Alert Description:**
  - The account [redacted] added an authentication me...
  - The operation attempted was SUCCESS
  - The authentication method registered was: User regist...
  - This type of authentication method was seen assigned t...
  - The IP used was [redacted]
  - The operation was performed from the ASN 42831, this...
  - These characteristics flagged this operation as unusual
- Alert name:** Suspicious authentication method addition to ...
- Alert severity:** Low
- Activity time:** [redacted]
- Alert category:** Persistence
- MITRE ATT&CK:** TA0003, T1078

The main area features a diagram with two nodes: a device icon on the left and a user icon on the right, connected by a dashed line. A red triangle with the letter 'A' is positioned above the user icon. Below the diagram, the alert title is 'Alert Suspicious authentication method addition to Azure account'. A table at the bottom shows the alert details:

TIMESTAMP	HOST	USER NAME	SEVERITY
[redacted]	[redacted]	[redacted]	Low

Figura 5 – Adição de método suspeito aos detalhes de alerta da conta do Azure.



## 2 MITRE ATT&CK - TTPs

---

<b>Tática</b>	<b>Técnica</b>	<b>Detalhes</b>
Initial Access	<a href="#">T1078.002</a>	Consiste em técnicas que usam vários vetores de entrada para ganhar sua posição inicial dentro de uma rede.
Resource Development	<a href="#">T1586</a>	Consiste em técnicas que envolvem adversários criando, comprando ou comprometendo/roubando recursos que podem ser usados para dar suporte à segmentação.
Persistence	<a href="#">TA0003</a>	Consiste em técnicas que os adversários usam para manter o acesso aos sistemas em reinicializações, credenciais alteradas e outras interrupções que podem cortar seu acesso.
Command and Control	<a href="#">TA0011</a>	Consiste em técnicas que adversários podem usar para se comunicar com sistemas sob seu controle dentro de uma rede de vítima.

*Tabela 1 – Tabela MITRE ATT&CK.*

### 3 RECOMENDAÇÕES

---

Além dos indicadores de comprometimento elencados abaixo pela ISH, poderão ser adotadas medidas visando a mitigação da infecção do referido *malware*, como por exemplo:

#### **Verifique a URL do site**

- Certifique-se de que o site que você está acessando é legítimo. Verifique se o endereço começa com "https://" e procure por erros de digitação no URL.

#### **Desconfie de pedidos urgentes de informações**

- E-mails ou mensagens que solicitam informações pessoais ou financeiras com urgência são suspeitos. Empresas legítimas raramente pedem esse tipo de informação dessa maneira.

#### **Não confie em janelas pop-up**

- Evite inserir informações pessoais em janelas pop-up. Feche-as e acesse o site diretamente pelo navegador.

#### **Use autenticação de dois fatores (2FA)**

- Adicione uma camada extra de segurança às suas contas, utilizando a autenticação de dois fatores sempre que possível.

#### **Mantenha seu software atualizado**

- Atualize regularmente seu sistema operacional, navegadores e programas de segurança para proteger-se contra vulnerabilidades conhecidas.

#### **Estabeleça políticas de segurança e privacidade**

- Se você gerencia uma empresa, implemente políticas claras de segurança e privacidade para todos os funcionários.

#### **Eduque-se e eduque os outros**

- Mantenha-se informado sobre as últimas técnicas de phishing e compartilhe esse conhecimento com colegas e familiares.

## 4 INDICADORES DE COMPROMETIMENTO (IoC)

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 Comprometimento (IOCs) relacionadas a análise do(s) artefato(s) deste relatório.

### Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
<b>URL</b>	<p> <a href="https://share-eu1.hsforms.com/1P_6lFHnbRriC_DG56YzVhw2dz72l">https://share-eu1.hsforms.com/1P_6lFHnbRriC_DG56YzVhw2dz72l</a>  <a href="https://share-eu1.hsforms.com/1UgPJ18suRU-NEpmYkEwteg2ec0io">https://share-eu1.hsforms.com/1UgPJ18suRU-NEpmYkEwteg2ec0io</a>  <a href="https://share-eu1.hsforms.com/12-j0Y4sfQh-4pEV6VKVOeg2dzmbq">https://share-eu1.hsforms.com/12-j0Y4sfQh-4pEV6VKVOeg2dzmbq</a>  <a href="https://share-eu1.hsforms.com/1wg25r1Z-R5GkhY6k-xGzOg2dvcv5">https://share-eu1.hsforms.com/1wg25r1Z-R5GkhY6k-xGzOg2dvcv5</a>  <a href="https://share-eu1.hsforms.com/1G-NQN9DbSVmDy1HDeovJCQ2ebgc6">https://share-eu1.hsforms.com/1G-NQN9DbSVmDy1HDeovJCQ2ebgc6</a>  <a href="https://share-eu1.hsforms.com/1AEc2-gS4TuyQyAiMQfB5Qw2e5xq0">https://share-eu1.hsforms.com/1AEc2-gS4TuyQyAiMQfB5Qw2e5xq0</a>  <a href="https://share-eu1.hsforms.com/1wg25r1Z-R5GkhY6k-xGzOg2dvcv5">https://share-eu1.hsforms.com/1wg25r1Z-R5GkhY6k-xGzOg2dvcv5</a>  <a href="https://share-eu1.hsforms.com/1QPAfZcocSuu3AnqznjU14A2eabj0">https://share-eu1.hsforms.com/1QPAfZcocSuu3AnqznjU14A2eabj0</a>  <a href="https://share-eu1.hsforms.com/176T8k3N9Q562OEEfhS22Fg2ebzvj">https://share-eu1.hsforms.com/176T8k3N9Q562OEEfhS22Fg2ebzvj</a>  <a href="https://share-eu1.hsforms.com/18wO3Zb9hTluttmhHvQFuQ2ec8gt">https://share-eu1.hsforms.com/18wO3Zb9hTluttmhHvQFuQ2ec8gt</a>  <a href="https://share-eu1.hsforms.com/1vNr8tB1GS4mZuYg81ji3dgd2e08a3">https://share-eu1.hsforms.com/1vNr8tB1GS4mZuYg81ji3dgd2e08a3</a>  <a href="https://share-eu1.hsforms.com/1qe8ypRpdTr284rkNpgmoow2ebzty">https://share-eu1.hsforms.com/1qe8ypRpdTr284rkNpgmoow2ebzty</a>  <a href="https://technicaldevelopment.rljaccommodationstrust.com/buzz/?WKg=2Ljv8">https://technicaldevelopment.rljaccommodationstrust.com/buzz/?WKg=2Ljv8</a>  <a href="https://asdrfghjk3wr4e5yr6uyjhgb.mhp-hotels.com/buzz/?Nhv3zM=xI7Kyf">https://asdrfghjk3wr4e5yr6uyjhgb.mhp-hotels.com/buzz/?Nhv3zM=xI7Kyf</a>  <a href="https://asdrfghjk3wr4e5yr6uyjhgb.mhp-hotels.com/buzz/?Nhv3zM=xI7Kyf">https://asdrfghjk3wr4e5yr6uyjhgb.mhp-hotels.com/buzz/?Nhv3zM=xI7Kyf</a>  <a href="https://orderconfirmation.dgpropertyconsultants.com/buzz/">https://orderconfirmation.dgpropertyconsultants.com/buzz/</a>  <a href="https://technicaldevelopment.industrialization.com/buzz/?oOB=RLNT">https://technicaldevelopment.industrialization.com/buzz/?oOB=RLNT</a>  <a href="https://docs.doc2rprevn.com/buzz?username=">https://docs.doc2rprevn.com/buzz?username=</a>  <a href="https://sensational-valkyrie-686c5f.netlify.com/app/?e=">https://sensational-valkyrie-686c5f.netlify.com/app/?e=</a> </p>
<b>IP</b>	<p>           167[.]114.27[.]228            144[.]217.158[.]133            91[.]92.245[.]39            91[.]92.244[.]131            91[.]92.253[.]66            94[.]156.71[.]208            91[.]92.242[.]68            91[.]92.253[.]66            188[.]166.3[.]116            74[.]119.239[.]234            208[.]91.198[.]96            94[.]46.246[.]46         </p>

Tabela 2 – Indicadores de Comprometimento de Rede.

Obs: Os *links* e endereços IP elencados acima podem estar ativos; cuidado ao realizar a manipulação dos referidos IoCs, evite realizar o clique e se tornar vítima do conteúdo malicioso hospedado no IoC.

## 5 REFERÊNCIAS

---

- Heimdall *by* ISH Tecnologia
- [Unit42](#)
- [Bleepingcomputer](#)

## 6 AUTORES

---

- Leonardo Oliveira Silva



heimdall  
security research

A DIVISION OF ISH