# BOLETIM DE SEGURANÇA

## Campanha ArcaneDoor explorando vulnerabilidades Zero Days da Cisco

heimdall
security research
A DIVISION OF ISH

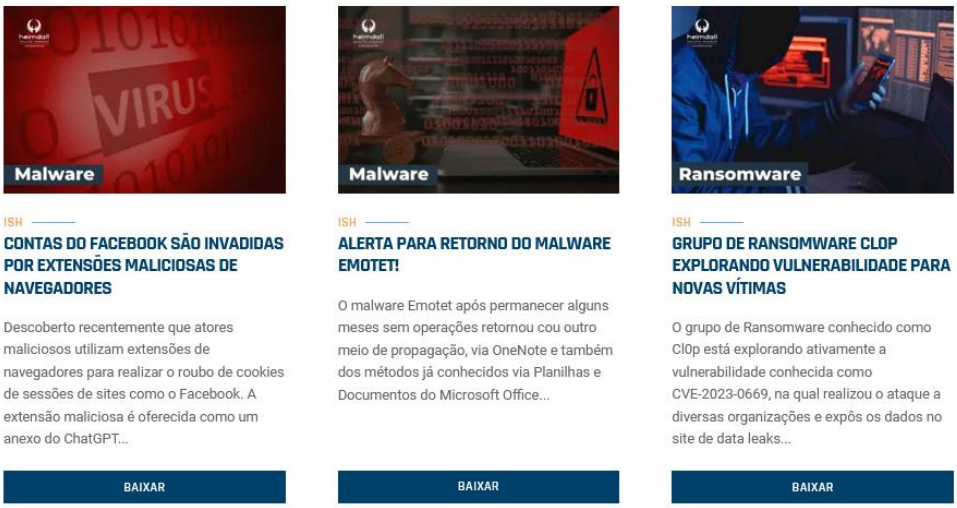
**TLP: CLEAR**

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 Cisco Talos emitiu um alerta sobre um grupo de ciberespionagem que, desde novembro de 2023, tem explorado vulnerabilidades inéditas nos firewalls ASA e FTD para comprometer redes governamentais globais. Os invasores, conhecidos como UAT4356 e STORM-1849, iniciaram ataques aos dispositivos vulneráveis com a campanha ArcaneDoor. A Cisco ainda investiga o vetor inicial de ataque, mas já remediou duas vulnerabilidades críticas, CVE-2024-20353 e CVE-2024-20359, exploradas pelos hackers como zero day.

# 2 INFORMAÇÃO SOBRE A AMEAÇA

A campanha ArcaneDoor representa o mais recente esforço de entidades estatais em direcionar dispositivos de rede perimetral de diversos fabricantes, visando a espionagem. Esses dispositivos são essenciais para a segurança da rede, pois controlam o fluxo de dados e, se comprometidos, permitem aos invasores se infiltrarem nas organizações, manipularem o tráfego e monitorarem as comunicações. Nos últimos anos, houve um aumento significativo no ataque a esses dispositivos, especialmente em setores críticos como telecomunicações e energia, que são alvos estratégicos para governos estrangeiros.

Em 2024, a Cisco alertou sobre possíveis vulnerabilidades em seus dispositivos ASA. A Talos, juntamente com a equipe PSIRT, iniciou uma investigação que revelou a atuação do grupo UAT4356, também conhecido como STORM-1849 pela Microsoft. Este grupo utilizou ferramentas avançadas e táticas de espionagem, demonstrando um alto nível de sofisticação e conhecimento dos dispositivos alvo. Durante a campanha ArcaneDoor, o UAT4356 implementou dois backdoors, "Line Runner" e "Line Dancer", para realizar atividades maliciosas, incluindo alterações de configuração, reconhecimento, captura e exfiltração de dados, e possíveis movimentos laterais na rede da vítima.

No começo de 2024, detectou-se atividades atípicas em um de seus dispositivos ASA. A investigação subsequente revelou mais vítimas, envolvendo redes governamentais globais. Descobriu-se que a infraestrutura dos atacantes estava ativa desde novembro de 2023, com picos de atividade entre dezembro de 2023 e janeiro de 2024. Evidências indicam que os atacantes já testavam e aprimoravam suas capacidades desde julho de 2023.

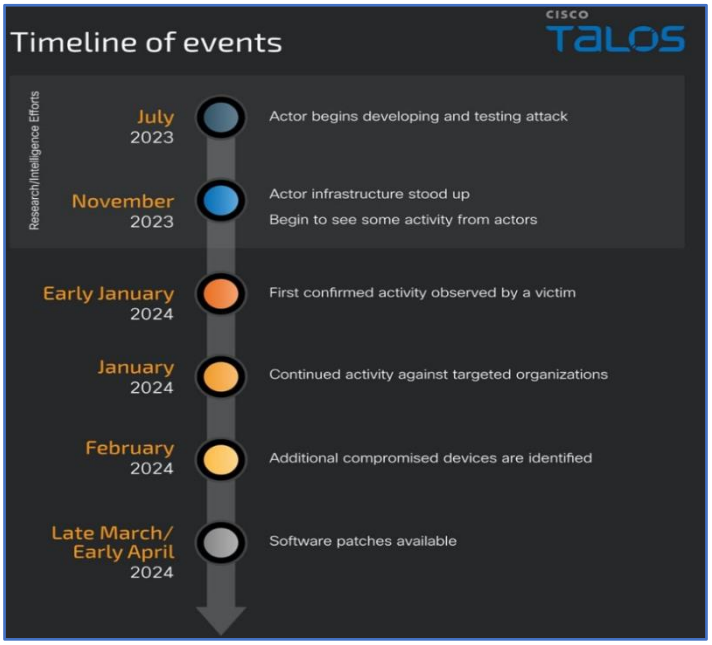



*Figura 1 – Timeline dos eventos.*

Nesta campanha, foram exploradas duas falhas de segurança (CVE-2024-20353 e CVE-2024-20359), com correções detalhadas nos comunicados de segurança da Cisco. O método inicial de intrusão ainda não foi identificado.

O Line Dancer, é um implante que opera diretamente na memória, atuando como um interpretador de shellcode, permitindo a execução de códigos arbitrários pelos atacantes. Nos dispositivos ASA afetados, o shellcode é transmitido através do campo Host-scan-reply, processado pelo Line Dancer, sem indicar a exploração do CVE-2018-0101. Esse campo é normalmente empregado em etapas avançadas da sessão SSL VPN e é interpretado por dispositivos ASA com configurações específicas para SSL VPN, IPsec IKEv2 VPN com serviços de cliente ou acesso de gerenciamento HTTPS. Ele é utilizado para realizar comandos no dispositivo invadido. Observou-se o seu uso para fins como, desativar o syslog, executar e extrair o comando show configuration, criar e extrair capturas de pacotes, executar comandos CLI contidos no shellcode, incluindo comandos de modo de configuração e a habilidade de salvá-los na memória (write mem), interromper o processo de despejo de memória, evitando a análise forense, pois o crash dump conteria evidências do comprometimento, manipular a função AAA (Autenticação, Autorização e Contabilidade) para habilitar uma autenticação especial. Isso permite ao invasor estabelecer um túnel VPN de acesso remoto usando um "número mágico", contornando os mecanismos AAA. Alternativamente, um blob P12 e um certificado associado são gerados e exfiltrados, junto com uma configuração de túnel baseada em certificado.

Dentro do processo de memória do Line Dancer, foi identificada uma função que verifica um token de 32 bytes contra um padrão. Se correspondente, decodifica a carga em base64, transfere para uma área de memória executável e invoca a função decodificada, finalizando com a chamada a função processHostScanReply(). Essa função é normalmente acessada por um ponteiro de função na tabela elementArray, associado à string host-scan-reply. Na memória capturada, a entrada que deveria apontar para processHostScanReply() agora direciona para a função do invasor que decodifica e executa a carga útil. Essa modificação, por estar na seção de dados da memória, não é refletida em hashes ou despejos de texto. A função do invasor opera da seguinte maneira:

```
{
long payload;
int iVar2;
uint len;
void *decoded_payload;
if (ip_pak != 0) {
payload = ip_pak + 0x20; iVar2 =
memcmp(s_                                    _55824e200200,ip_pak,0x2
0); if (iVar2 == 0) {
len = __wrap_strlen(payload); decoded_payload = malloc(len);
if (decoded_payload != (void *)0x0) {
base64_decode(payload,decoded_payload);
memcpy(CUS_shellcode_payload,decoded_payload,(ulong)len);
free(decoded_payload);
CUS_shellcode_payload();
} }
} processHostScanReply(param_1); return;
}
```

*Figura 2 – função processHostScanReply().*

Para manter a persistência no dispositivo ASA comprometido, o agente de ameaça emprega um segundo backdoor duradouro denominado "Line Runner". Este backdoor aproveita uma funcionalidade antiga que facilitava o carregamento antecipado de clientes VPN e plug-ins no aparelho. Durante o processo de inicialização, o ASA é configurado para verificar se há um arquivo específico em **disco0:**, utilizando uma expressão regular Lua para essa busca.

```
^client_bundle[%w_-]*%.zip$
```

*Figura 3 – Expressão regular.*

Caso detectado, o arquivo em questão é extraído e o script **csco_config.lua** é executado. Após a execução, o arquivo ZIP é removido. Esse procedimento está associado ao CVE-2024-20359, com informações adicionais disponíveis no Cisco Security Advisory. Adicionalmente, foi identificada outra falha de segurança, CVE-2024-20353, que foi explorada para auxiliar nesse processo. Utilizando essa brecha, os atacantes induziram a reinicialização do dispositivo ASA visado, o que desencadeou a extração e ativação do Line Runner, o segundo elemento do malware implantado.

Os componentes contidos no arquivo ZIP do malware incluem:

```
./csco_config.lua
./csco_config2.lua
./client_bundle_install/plugin/rdp.jar
./client_bundle_install/test/stgvdr.txt
./client_bundle_install/test/index.txt
./client_bundle_install/test/hash.txt
./client_bundle_install/test/umtfc.txt
./client_bundle_install/test/laecsnw.txt
```

*Figura 4 – Componentes do malware.*

Os scripts contidos no arquivo zip conferem ao agente da ameaça um backdoor Lua persistente via HTTP no ASA, que se mantém ativo mesmo após reinicializações e atualizações. O Line Runner, utilizado pelo UAT4356, serve para extrair informações previamente processadas pelo Line Dancer.

Este script csco_config.lua é executado durante a inicialização do sistema e realiza as ações de criar o diretório '**disk0:/csco_config/97/webcontent**' caso não exista. Gera o arquivo '**disk0:/csco_config/97/webcontent/1515480F4B538B669648B17C02337098'** a partir do '**hash.txt**', concatena '**index.txt**' ao '**disk0:/csco_config/97/webcontent/index_bp.ini**' e salva o resultado em '**disk0:/csco_config/97/webcontent/index.ini**'. Em seguida transfere o arquivo '**client_bundle.zip**' para **'/run/lock/subsys/krbkdc6'**, inserindo **'umtfc.txt'** no início de **'/etc/init.d/umountfs'**. Copia **'stgvdr.txt'** para **'/asa/scripts/lina_cs'**. Realiza backup de **'/asa/scripts/lina_exe_cs.sh'** para **'/asa/scripts/lina_exe_cs_bp.sh'**. Depois substitui **'/asa/scripts/lina_exe_cs.sh'** por **'laecsnw.txt'**. Copia **'csco_config2.lua'** para **'csco_config.lua'**. Desativa temporariamente a função **'importPlugin'**.

Para identificar a presença do Line Runner em um ASA, após a atualização do dispositivo para uma versão de software com correção para o CVE-2024-20359, deve-se revisar o conteúdo do **'disk0:'**. A aparição de um novo arquivo **'.zip'** sugere a presença anterior do Line Runner. Com o software atualizado, o Line Runner fica inativo. Uma série de comandos cria um arquivo **'.zip'** inofensivo que será lido pelo ASA na reinicialização. Se um novo arquivo **'.zip'** surgir no **'disk0:'** após a recarga, indica a presença do Line Runner. A exclusão do arquivo **'client_bundle_install.zip'** remove o Line Runner. O arquivo malicioso pode ter outros nomes seguindo o padrão.

```
asa> enable
asa# show version | redirect disk0:/client_bundle.zip
asa# show disk0:
# ... Verify `client_bundle.zip` is present
asa# reload
# ... Device reboots
asa> enable
asa# show disk0:
# ... If the device had the persistence mechanism in place
# ... a new file `client_bundle_install.zip` will be present on disk0:
# ... Suggest retrieving and then deleting `client_bundle_install.zip`
# ... from disk0:
```

*Figura 5 – Comandos que criará um arquivo .zip.*

O UAT4356 adotou estratégias específicas para obstruir a análise forense de componentes mal-intencionados, revelando um entendimento profundo do ASA e dos procedimentos forenses padrão da Cisco para verificar a integridade dos dispositivos de rede.

Foram implementadas medidas pontuais para camuflar atividades no aparelho, incluindo a manipulação da função AAA (Autenticação, Autorização e Contabilidade) para contornar os processos normais de AAA. Observou-se que, em certos casos, o UAT4356 desativou o registro de logs para realizar tarefas no ou através do ASA sem deixar rastros.

Na investigação, foi avaliada a autoria do incidente, baseando na vitimologia, no elevado grau de competência no desenvolvimento de ferramentas e táticas anti-forenses, e na exploração e ligação de vulnerabilidades zero-day. Com base nesses elementos, foi concluída que as ações foram executadas por um agente apoiado por um Estado.

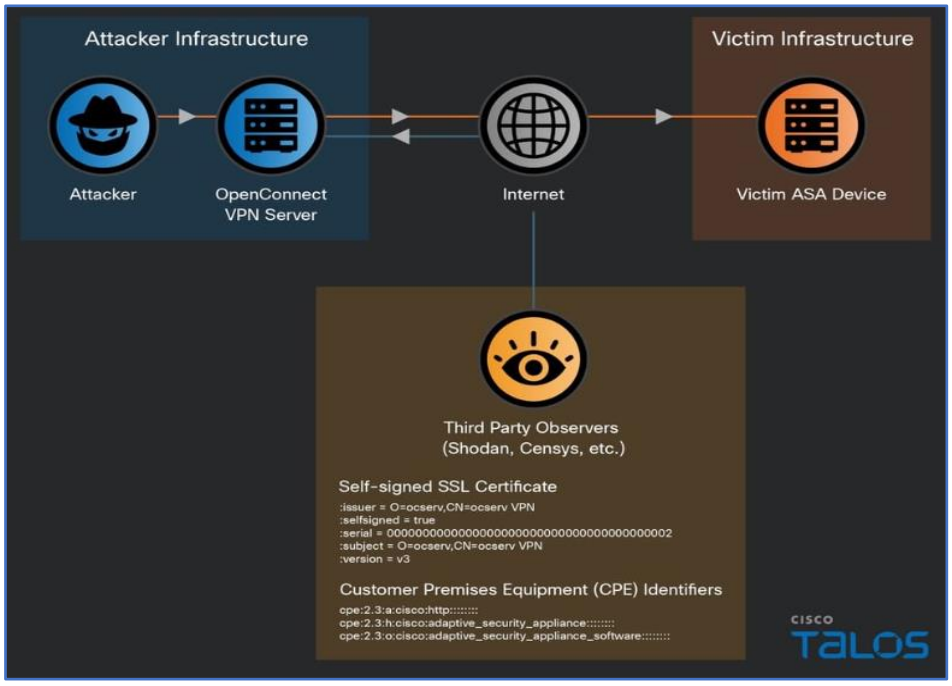
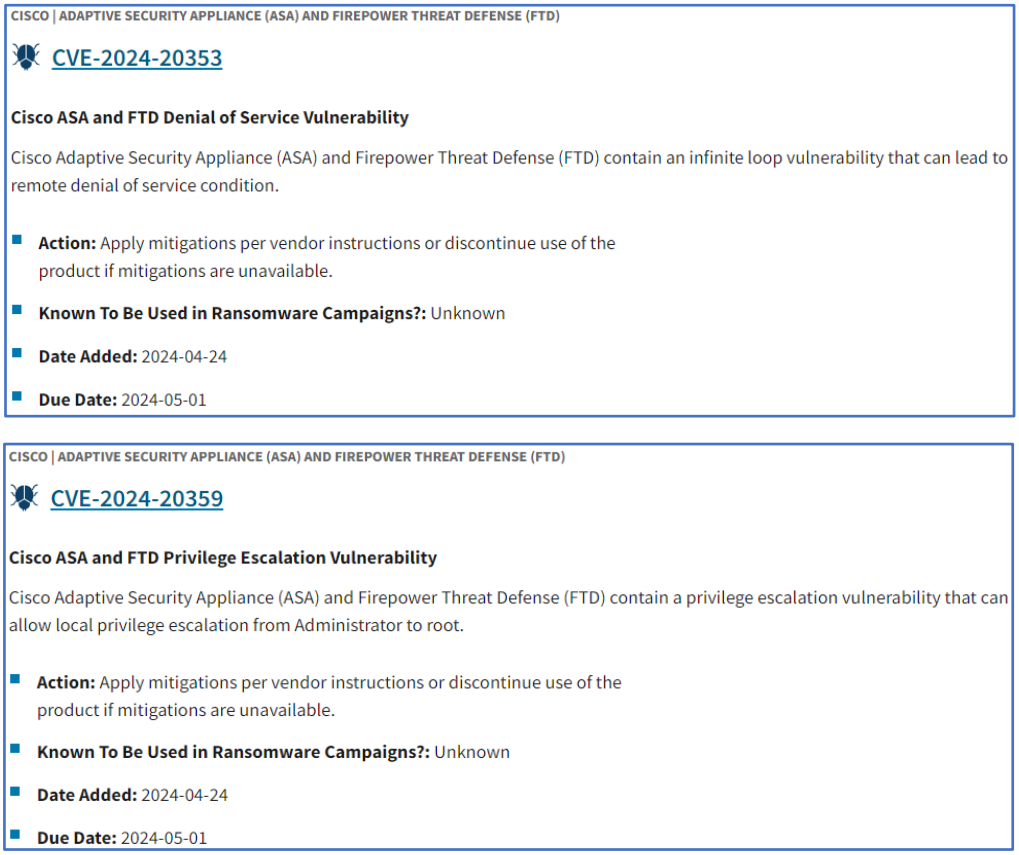



*Figura 6 – Infraestrutura UAT4356.*

# 3 VULNERABILIDADES ADICIONADAS AO KEV-CISA

A agência de segurança cibernética (CISA) adicionou as falhas ao seu Catálogo de Vulnerabilidades Exploradas Conhecidas (KEV), dizendo que tais vulnerabilidades são “vetores de ataque frequentes para atores cibernéticos maliciosos”.



CISCO | ADAPTIVE SECURITY APPLIANCE (ASA) AND FIREPOWER THREAT DEFENSE (FTD)

CVE-2024-20353

**Cisco ASA and FTD Denial of Service Vulnerability**

Cisco Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) contain an infinite loop vulnerability that can lead to remote denial of service condition.

- **Action:** Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
- **Known To Be Used in Ransomware Campaigns?:** Unknown
- **Date Added:** 2024-04-24
- **Due Date:** 2024-05-01

CISCO | ADAPTIVE SECURITY APPLIANCE (ASA) AND FIREPOWER THREAT DEFENSE (FTD)

CVE-2024-20359

**Cisco ASA and FTD Privilege Escalation Vulnerability**

Cisco Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) contain a privilege escalation vulnerability that can allow local privilege escalation from Administrator to root.

- **Action:** Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
- **Known To Be Used in Ransomware Campaigns?:** Unknown
- **Date Added:** 2024-04-24
- **Due Date:** 2024-05-01

*Figura 7 – Vulnerabilidades no catálogo KEV-CISA.*

# 4 MITRE ATT&CK - TTPs

| Tática | Técnica | Detalhes |
|---|---|---|
| **Persistence** | T1037<br>T1653<br>T1556 | A persistência consiste em técnicas que os adversários usam para manter o acesso aos sistemas após reinicializações, alterações de credenciais e outras interrupções que podem interromper seu acesso. |
| **Defense Evasion** | T1140<br>T1562.001<br>T1070.004 | A Evasão de Defesa consiste em técnicas que os adversários usam para evitar a detecção durante todo o seu comprometimento. |
| **Execution** | T0874<br>T1059 | A execução consiste em técnicas que resultam na execução de código controlado pelo adversário em um sistema, dispositivo ou outro ativo local ou remoto. |
| **Privilege Escalation** | T1055 | O escalonamento de privilégios consiste em técnicas que os adversários usam para obter permissões de nível superior em um sistema ou rede. |
| **Credential Access** | T1557<br>T1040 | O Credential Access consiste em técnicas para roubar credenciais, como nomes de contas e senhas. |
| **Command and Control** | T1071.001<br>T1102.003 | Comando e Controle consiste em técnicas que os adversários podem usar para se comunicar com sistemas sob seu controle dentro de uma rede vítima. |
| **Exfiltration** | T1041 | A exfiltração consiste em técnicas que os adversários podem usar para roubar dados da sua rede. |

Tabela 1 – Tabela MITRE ATT&CK.

# 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:

**Atualize regularmente o software**

- Mantenha todos os sistemas operacionais e softwares atualizados com as últimas versões e patches de segurança.

**Use antivírus e firewalls**

- Instale e mantenha atualizados programas antivírus e firewalls para detectar e bloquear software malicioso e acessos não autorizados.

**Crie backups**

- Faça backups regulares de dados importantes para poder recuperá-los em caso de ataque cibernético ou falha do sistema.

**Treinamento de conscientização**

- Eduque os usuários sobre os riscos de segurança e boas práticas, como não clicar em links suspeitos ou abrir anexos de e-mails não confiáveis.

**Controle de acesso**

- Implemente políticas de controle de acesso para restringir o acesso a informações sensíveis apenas a usuários autorizados.

**Autenticação forte**

- Utilize métodos de autenticação multifator para adicionar uma camada extra de segurança ao acessar sistemas críticos.

**Monitoramento e resposta a incidentes**

- Monitore redes e sistemas em busca de atividades suspeitas e tenha um plano de resposta a incidentes para agir rapidamente em caso de violação de segurança.

# 6 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 URL, IPs e Domínios**

| Indicadores de URL, IPs e Domínios | |
|---|---|
| IP | 192.36.57[.]181<br>185.167.60[.]85<br>185.227.111[.]17<br>176.31.18[.]153<br>172.105.90[.]154<br>185.244.210[.]120<br>45.86.163[.]224<br>172.105.94[.]93<br>213.156.138[.]77<br>89.44.198[.]189<br>45.77.52[.]253<br>103.114.200[.]230<br>212.193.2[.]48<br>51.15.145[.]37<br>89.44.198[.]196<br>131.196.252[.]148<br>213.156.138[.]78<br>121.227.168[.]69<br>213.156.138[.]68<br>194.4.49[.]6<br>185.244.210[.]65<br>216.238.75[.]155<br>5.183.95[.]95<br>45.63.119[.]131<br>45.76.118[.]87 |

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.

Se deseja ter acesso aos demais Indicadores de Compromissos (IoCs), envie um e-mail para: heimdall@ish.com.br

# 7 REFERÊNCIAS


- **Heimdall *by* ISH Tecnologia**
- Cisco_Talos
- Bleppingcomputer
- NVD

heimdall
security research
A DIVISION OF ISH