TLP: CLEAR

BOLETIM DE SEGURANÇA

Androxgh0st Botnet: Ameaça global a dispositivos IoT

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

SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

1 INFORMAÇÕES SOBRE A BOTNET ANDROXGHOST

Pesquisadores da CloudSEK detectaram avanços preocupantes relacionados à botnet **Androxgh0st**, destacando sua capacidade de explorar múltiplas vulnerabilidades e sua possível integração com a botnet Mozi. Desde janeiro de 2024, o Androxgh0st tem como alvo principal servidores web. No entanto, registros recentes de servidores de comando e controle (C2) apontam para a implantação de payloads Mozi focados em dispositivos IoT. A CISA já havia emitido um alerta sobre essa botnet no início do ano. Androxgh0st afeta tecnologias como Cisco ASA, Atlassian JIRA e frameworks PHP, permitindo acesso não autorizado e execução remota de código. Esse comportamento reflete uma intensificação nas operações dos operadores da botnet, que agora exploram uma gama mais ampla de vulnerabilidades.

Conforme análise, foi revelado que o Androxgh0st tem explorado mais de 20 vulnerabilidades desde agosto de 2024. A CISA, em janeiro de 2024, publicou um comunicado sobre o crescimento dessa botnet e seus vetores de ataque inicial:

- Exploração do PHP no PHPUnit (CVE-2017-9841): Essa vulnerabilidade é explorada em pastas expostas de frameworks PHP, como **/vendor**, utilizando páginas específicas para executar código remotamente e inserir arquivos maliciosos, garantindo acesso backdoor.
- Arquivos.env no Laravel Framework (CVE-2018-15133): A botnet busca arquivos.env do Laravel para roubar credenciais e explorar chaves de aplicação, permitindo execução de código remoto e uploads de arquivos maliciosos.
- Path Traversal no Apache (CVE-2021-41773): Em versões específicas do Apache, agentes exploram configurações incorretas para acessar arquivos fora do diretório raiz e executar código arbitrário, comprometendo dados confidenciais.

A botnet Androxgh0st tem infectado um número crescente de dispositivos diariamente. Atualmente, mais de 500 dispositivos já foram comprometidos. Essaexpansão demonstra a rápida disseminação da ameaça, reforçando a necessidade de medidas preventivas imediatas.

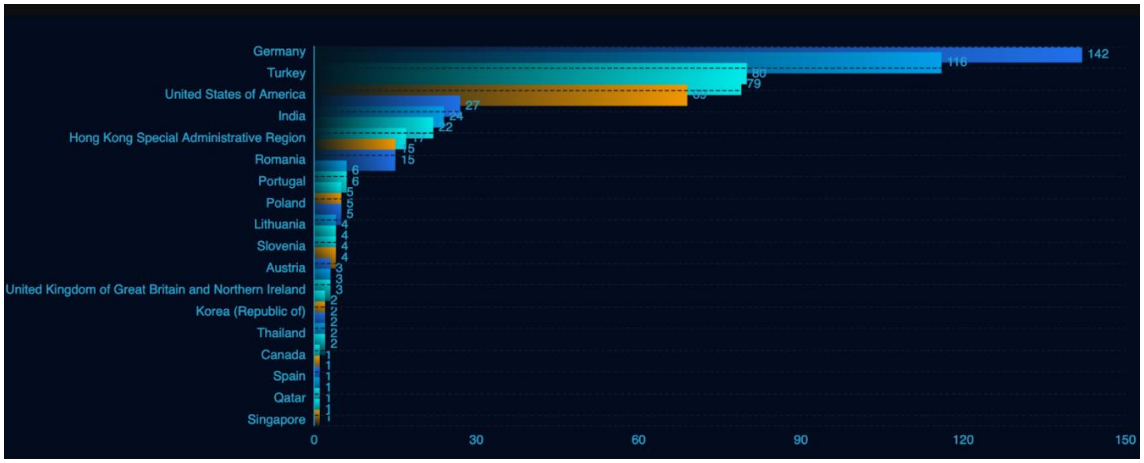

Figura 1 – Bots por país.

A análise identificou uma série de vulnerabilidades críticas. Essas falhas estão sendo ativamente exploradas pela botnet Androxgh0st para comprometer sistemas e obter acesso inicial.

PRODUTO AFETADO	IMPACTO
Cisco ASA (até 8.4.7/9.1.4) - CVE-2014-2120	Injeção arbitrária de script web ou HTML por meio de um parâmetro não especificado.
Atlassian JIRA (antes da versão 8.5.14, da versão 8.6.0 antes da 8.13.6 e da versão 8.14.0 antes da 8.16.1) - CVE-2021-26086	Permite que invasores remotos leiam arquivos específicos por meio de uma vulnerabilidade de path traversal no endpoint /WEB-INF/web.xml.
Versões do Metabase GeoJSON x.40.0-x.40.4 - CVE-2021-41277	Um invasor remoto não autenticado pode explorar isso por meio de uma solicitação HTTP GET especialmente criada para baixar arquivos arbitrários com privilégios de root e examinar variáveis de ambiente.
Sophos Firewall versão v18.5 MR3 e anteriores - CVE-2022-1040	Um invasor remoto e não autenticado pode executar código arbitrário remotamente.
Oracle EBS versões 12.2.3 até 12.2.11 - CVE-2022-21587	Upload de arquivo arbitrário não autenticado
OptiLink ONT1GEW GPON 2.1.11_X101 Compilação 1127.190306	Execução de Remote Code Execution
PHP CGI (versões PHP 8.1.* antes de 8.1.29, 8.2.* antes de 8.2.20, 8.3.* antes de 8.3.8) - CVE-2024-4577	Permite que um invasor escape da linha de comando e passe argumentos para serem interpretados diretamente pelo PHP.
TP-Link Archer AX21 - CVE-2023-1389	Permite a execução de comandos não autenticados como root por meio do parâmetro country em /cgi-bin/luci;stok=/locale.
Imagem de fundo do plugin Wordpress Cropper v1.2	Remote Code Execution
Dispositivos Netgear DGN (Netgear DGN1000, versão de firmware < 1.1.00.48, Netgear DGN2200 v1)	Execução de comando não autenticado com privilégios de root

Roteadores GPON Home - CVE-2018-10561, CVE-2018-10562	Execução de comando não autenticado
ShopXO Download - CNVD-2021-15822	Leitura arbitrária de arquivo - Divulgação de informações confidenciais
ZenTao CMS - CNVD-2022-42853	SQL Injection - Divulgação de informações confidenciais
Relatório AJ - CNVD-2024-15077	Bypass de autenticação - Execução remota de código
eYouMail - CNVD-2021-26422	Remote Code Execution
Leadsec VPN - CNVD-2021-64035	Leitura arbitrária de arquivo - Divulgação de informações confidenciais
EduSoho	Leitura arbitrária de arquivo - Divulgação de informações confidenciais
UFIDA NC BeanShell - CNVD-2021-30167	Remote Code Execution
OA E-Cology LoginSSO.jsp - CNVD-2021-33202	SQL Injection - Divulgação de informações confidenciais
Spring Cloud Gateway < 3.0.7 e < 3.1.1 Injeção de código - CVE-2022-22947	Remote Code Execution
Weaver OA XmlRpcServlet - CNVD-2022-43245	Leitura arbitrária de arquivo - Divulgação de informações confidenciais
Ruijie Smartweb	Senha Fraca - Controle de Conta de Convidado
Hongjing HCM - CNVD-2023-08743	SQL Injection - Divulgação de informações confidenciais
E-Cology V9 - CNVD-2023-12632	SQL Injection - Divulgação de informações confidenciais
Ruckus Wireless Admin through 10.4 - CVE-2023-25717	Remote Code Execution

Tabela 1 – Produtos afetados e seus impactos.

A botnet Androxgh0st aproveita essas vulnerabilidades para expandir sua rede de dispositivos comprometidos, utilizando técnicas avançadas de exploração automatizada. Além de possibilitar o acesso inicial, essas falhas são exploradas para realizar movimentos laterais dentro da infraestrutura alvo, permitindo ataques mais complexos, como exfiltração de dados e instalação de backdoors persistentes. A capacidade de personalizar os ataques para cada alvo torna essa botnet uma ameaça significativa, especialmente para organizações com sistemas desatualizados ou configurados incorretamente.

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:

Conscientização de usuários

- Treine usuários para reconhecer tentativas de phishing sofisticadas, incluindo ataques que imitam páginas de autenticação de dois fatores (2FA). Ensine a verificar URLs e evitar clicar em links desconhecidos.

Use ferramentas de detecção de endpoint

- Utilize software de Endpoint Detection and Response (EDR), capaz de identificar comportamentos anômalos, processos não autorizados e arquivos suspeitos associados a possíveis infecções, como o Androxgh0st.

Monitoramento e auditoria de logs de autenticação

- Inspecione logs de autenticação para detectar padrões suspeitos, como múltiplas tentativas de login falhadas ou logins em locais geográficos não usuais. Ataques de phishing frequentemente capturam credenciais para tentativas de login subsequentes.

Revisão de configurações de segurança de contas

- Implemente políticas de segurança que bloqueiem automaticamente contas após um número definido de tentativas de login falhadas e exija autenticação de múltiplos fatores em todos os sistemas críticos.

Monitoramento de tráfego de rede para domínios maliciosos

- Utilize sistemas de detecção de intrusão (IDS) e listas de bloqueio de domínios conhecidos por hospedar phishing-as-a-service. Monitore requisições DNS e conexões HTTP/S suspeitas que possam indicar ataques em andamento.

Atualização regular de sistemas e aplicações

- Garanta que todos os sistemas, especialmente servidores web e dispositivos de autenticação, estejam atualizados com os patches mais recentes para evitar que vulnerabilidades sejam exploradas em campanhas de phishing.

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	
File name:	**Hashes de arquivo - Exploração Androxgh0st TP-Link (md5)**
md5:	2403a89ab4ffec6d864ac0a7a225e99a
	d9553ca3d837f261f8dfda9950978a0a
	c8340927faaf9dccabb84a849f448e92
	a2021755d4d55c39ada0b4abc0c8bcf5
	c8340927faaf9dccabb84a849f448e92
	db2a59a1fd789d62858dfc4f436822d7
	dd5e7a153bebb8270cf0e7ce53e05d9c
	f75061ac31f8b67ddcd5644f9570e29b
	45b5c4bff7499603a37d5a665b5b4ca3
	6f8a79918c78280aec401778564e3345
	e3e6926fdee074adaa48b4627644fccb
	abab0da6685a8eb739027aee4a5c4eaa
	2938986310675fa79e01af965f4ace4f
	a6609478016c84aa235cd8b3047223eb
	3cb30d37cdfe949ac1ff3e33705f09e3
	0564f83ada149b63a8928ff7591389f3
	3d48dfd97f2b77417410500606b2ced6

File name:	**Hashes de arquivo - Exploração do Geoserver Androxgh0st**
md5:	74f85c38ff44ff3b85124caf555cec27
	6f5a16332cb0b8fc787f1b1d30f5857a

Tabela 2 – Indicadores de Comprometimento

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
Registrador de solicitações e remetente de comandos - Androxgh0st	
Domínios	Api[.]next[.]eventsrealm[.]com
IP	165.22.184[.]66
	45.55.104[.]59
	Exploração do roteador TP Link - Servidores de download
	45.202.35[.]24
	154.216.17[.]31
	Exploração do Geoserver - Servidores de download
	206.189.109[.]146
	149.88.44[.]159
	Exploração do roteador Netgear - Servidor de download
	200.124.241[.]140
	Exploração de roteador GPON - Servidor de download
	117.215.206[.]216
	Administrador sem fio Ruckus (CVE-2023-25717)
	45.221.98[.]117

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**
- **CloudSEK**
- **NVD**
- **HACKread**

5 AUTORES

- **Wesley Murat**

heimdall
security research
A DIVISION OF ISH