BOLETIM DE SEGURANÇA

Ator de ameaça TA588 realizando campanha contra América Latina

heimdall
security research
A DIVISION OF ISH

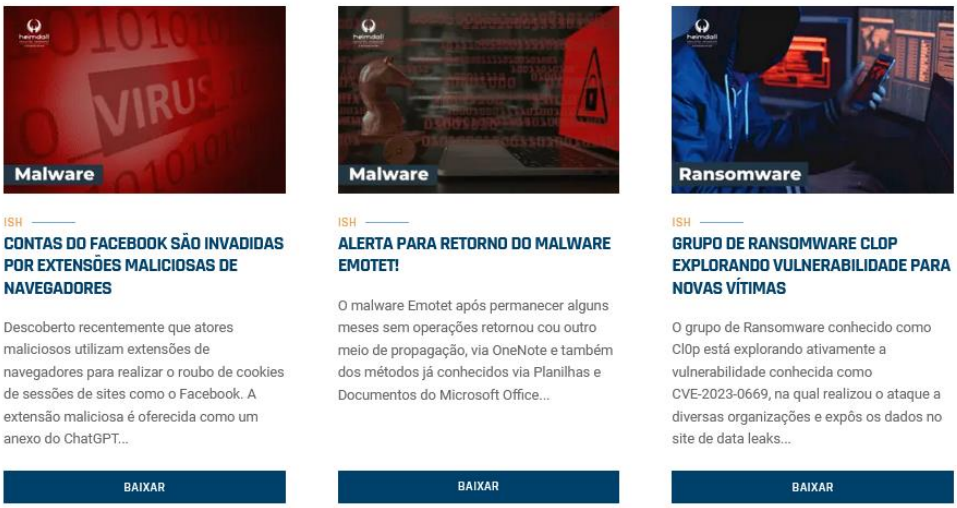
TLP: CLEAR

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

1 SUMÁRIO EXECUTIVO

Recentemente foi observado pelo pesquisador de ameaças **Idan Tarab**, que o grupo conhecido como **TA558**, especializado em ameaças cibernéticas, foi identificado como responsável por uma nova onda de ataques de phishing visando diversos setores na América Latina, com o objetivo de disseminar o Venom RAT.

Os alvos primários desses ataques incluem os setores de hotelaria, viagens, comércio, finanças, manufatura, indústria e governamentais em países como Espanha, México, Estados Unidos, Colômbia, Portugal, Brasil, República Dominicana e Argentina.

Ativo desde pelo menos 2018, o grupo TA558 possui um histórico de direcionar organizações na região latino-americana para implantar diversos tipos de malware, como Loda RAT, Vjw0rm e Revenge RAT. De acordo com as descobertas do pesquisador, a mais recente forma de infecção aproveita e-mails de phishing como meio de acesso inicial para distribuir o **Venom RAT**, uma variante do Quasar RAT que possui capacidades para coletar dados sensíveis e controlar sistemas de forma remota.

2 CONCLUSÃO

A ameaça do malware Venom RAT às organizações no Brasil destaca-se pela sua capacidade de controle remoto dos sistemas infectados, oferecendo aos cibercriminosos um arsenal para diversas atividades maliciosas, desde o furto de credenciais até a manipulação direta dos sistemas comprometidos. Distribuído principalmente através de e-mails spam e utilizando técnicas avançadas de ofuscação, este RAT complica a detecção e a análise por softwares de segurança. As organizações precisam estar especialmente atentas a essa ameaça, adotando medidas de segurança robustas.

3 MITRE ATT&CK - TTPs

Tática	Técnica	Detalhes
Initial Access	T1566.002	Spearphishing Link
Reconnaissance	T1590.005	Coleta de informações da rede da vítima, endereços IP.
Privilege Escalation, Defense Evasion	T1548.002	Abuso de mecanismo de controle de elevação.
Defense Evasion	T1562.001	Prejudicação de defesas, desativando ou modificando ferramentas.
Resource Development	T1584.005	Infraestrutura comprometida
Execution	T1059.007	Intérprete de comandos e scripts: JavaScript
Collection, Credential Access	T1056.001	Captura de entrada: Keylogging
Persistence, Privilege Escalation	T1547.001	Execução de inicialização automática de inicialização ou logon: chaves de execução do registro/pasta de inicialização.
Execution, Persistence, Privilege Escalation	T1053.005	Uso do agendador de tarefas
Persistence	T1136.002	Criação de conta: conta de domínio

Tabela 1 – Tabela MITRE ATT&CK.

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:

Educação e conscientização de funcionários

- Eduque os funcionários sobre as táticas de engenharia social usadas para distribuir malware, incluindo phishing e mal spam. Ensine-os a identificar e-mails suspeitos e a não clicar em links ou abrir anexos de remetentes desconhecidos.

Práticas de higiene cibernética

- Atualizações de segurança: Mantenha todos os sistemas e softwares atualizados. A instalação regular de patches de segurança é essencial para corrigir vulnerabilidades que podem ser exploradas por malwares como o Venom RAT.
- Controles de acesso rígidos: Aplique o princípio do menor privilégio, garantindo que os usuários tenham apenas os acessos necessários para realizar suas tarefas.

Ferramentas e soluções de segurança

- Antivírus e anti-malware: Utilize soluções robustas de antivírus e anti-malware, com atualizações automáticas e varreduras regulares para detectar e remover ameaças.
- Soluções de Endpoint Detection and Response (EDR): Implemente ferramentas de EDR para monitorar, detectar e responder a atividades suspeitas em endpoints de maneira proativa.
- Segurança de e-mail: Utilize gateways de e-mail seguros para filtrar ameaças antes que elas atinjam os usuários finais.

Detecção e Resposta

- Monitoramento e análise de logs: Configure a coleta e análise de logs para identificar comportamentos anormais que possam indicar a presença de RATs ou outras ameaças.
- Plano de resposta a incidentes: Desenvolva e teste um plano de resposta a incidentes cibernéticos, assegurando uma resposta rápida e eficaz a infecções por malware.

Tecnologias específicas

- Como o Venom RAT pode utilizar técnicas avançadas para evitar detecção, como a injeção em processos legítimos e o uso de comunicação

criptografada, a implementação de soluções que utilizam análise de comportamento e inteligência artificial pode oferecer detecção aprimorada.

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:	de2048e10e252a01bf6ca4e5a30f932c
sha1:	d0b49ad6cfd71d97688edeb57ccb37cd4e7e8480
sha256:	73725a049fd9de8bb148782333cb8bdcae43eb51347f4bf92dd28e74cd6b7229
File name:	Venombin.exe

Indicadores de compromisso do artefato	
md5:	25233DDA5807907C912C9B67779FFFF4
sha1:	05E57605A3733CF32CE5C667647816C5670DEB36
sha256:	2FEEC865DC334012E56E10F0458FD1DE60549E7B776F5B08F529D71C184FE79
File name:	JS.SAgent.

Tabela 2 – Indicadores de Compromissos de artefatos

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
Domínio	emailmarketing[.]locaweb[.]com.br
IP	68[.]178[.]203[.]123

Tabela 3 – 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**
- **Post Idan Tarab**
- **Mitre Att&ck**

heimdall
security research
A DIVISION OF ISH