BOLETIM DE SEGURANÇA

Os 07 tipos de malware mais comuns

heimdall
security research
A DIVISION OF ISH

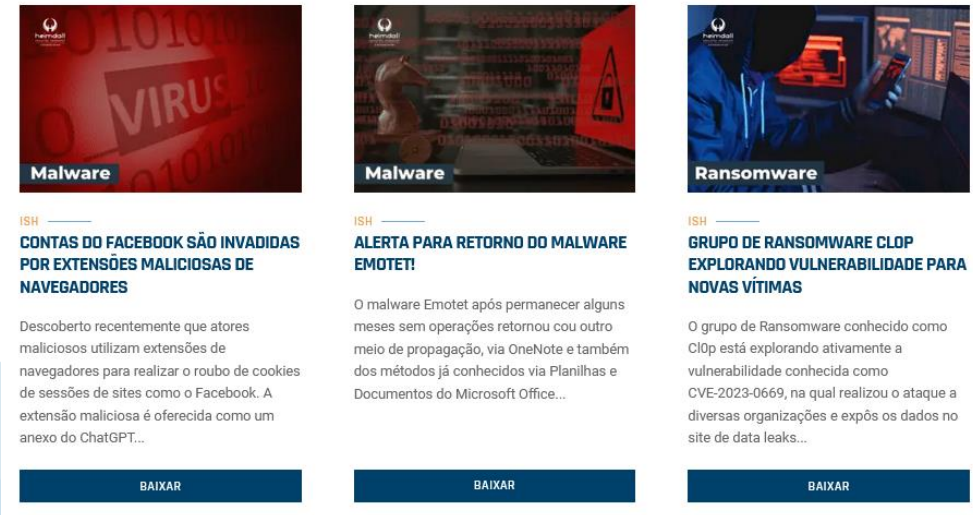
TLP: CLEAR

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso Twitter.

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

Sumário

1 Sumário executivo 5
2 Malwares identificados 6
3 Conclusão 11
4 Recomendações 12
5 Referências 14

Lista de Figuras

Figura 1 – Tipos mais comuns de malware do tipo Loader na base. 6

1 SUMÁRIO EXECUTIVO

Recentemente a ANY.RUN, uma plataforma de análise de malware que oferece um ambiente virtual para testar e investigar ameaças cibernéticas com a execução e observação de malwares, disponibilizou um relatório sobre os 07 principais tipos de malwares mais comuns em sua base, os quais serão apresentados logo mais neste boletim de segurança.

2 MALWARES IDENTIFICADOS

Com base na análise de sandbox ANY.RUN de milhares de envios diários, os tipos de malware mais comuns relatados são:

Malware Loader

Muitas vezes chamado de "***dropper***" ou "***downloader***", é um tipo de software malicioso projetado para baixar e instalar outro malware em um sistema comprometido. Ao contrário de muitas outras formas de malware, os carregadores normalmente não realizam eles próprios a principal atividade maliciosa. Em vez disso, sua função principal é estabelecer uma posição no sistema e, em seguida, recuperar malware adicional, muitas vezes mais destrutivo, de um servidor remoto.

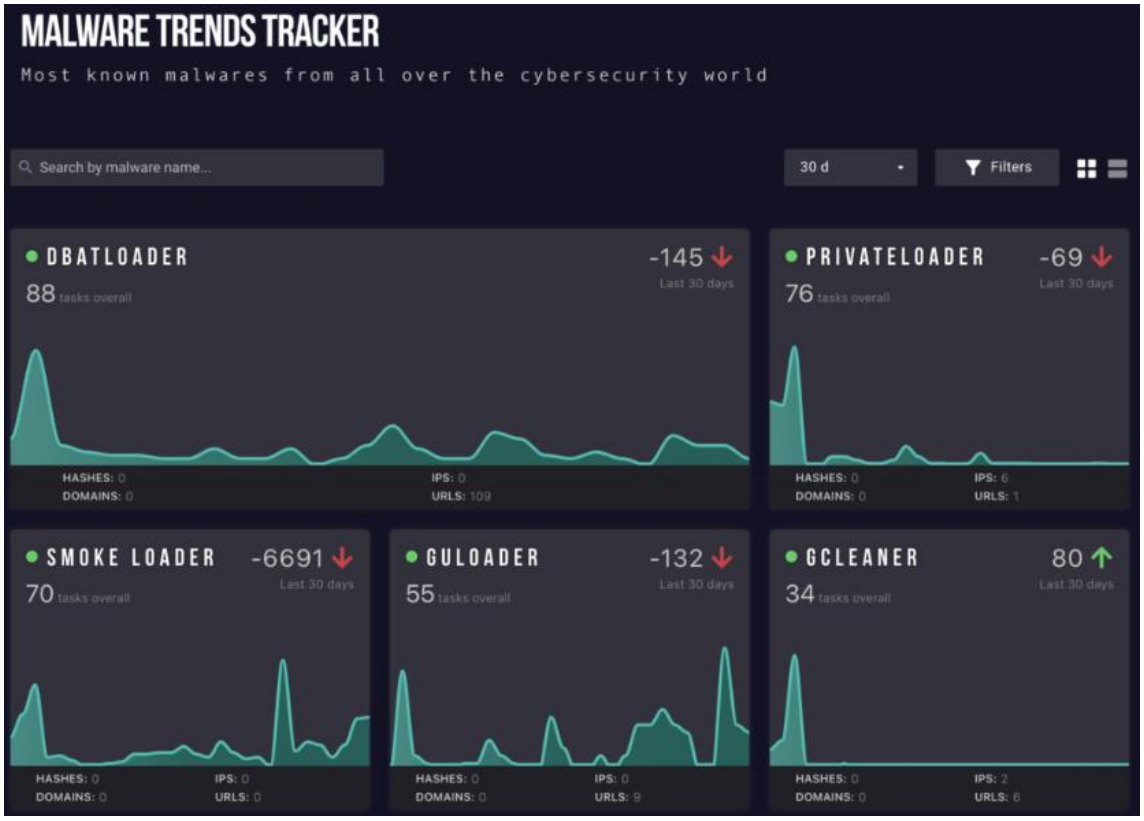


Figura 1 – Tipos mais comuns de malware do tipo Loader na base.

Os malwares do tipo Loader encontrados com mais frequência na plataforma foram os seguintes:

- **DBatLoader**
- **PrivateLoader**
- **Smoke Loader**
- **GULoader**
- **GCleaner**

Malware Stealer

Um tipo de software malicioso projetado para extrair informações confidenciais de sistemas infectados. Esta categoria de malware tem como alvo dados como credenciais, informações financeiras e dados pessoais, que podem incluir nomes de usuário, senhas, detalhes de cartão de crédito e outras informações privadas.

As principais características do malware Stealer incluem:

- **Extração de dados**: Sua principal função é roubar dados confidenciais de sistemas comprometidos.
- **Stealth**: Muitas vezes opera silenciosamente em segundo plano para evitar detecção.
- **Transmissão de dados roubados**: Os dados roubados geralmente são transmitidos de volta ao invasor para um servidor de comando e controle.
- **Múltiplas fontes de dados**: Os Stealers podem extrair dados de navegadores da web, sistemas de arquivos, sistemas FTP e outros softwares onde dados confidenciais podem ser armazenados.

Trojan de acesso remoto (RAT)

Este é um tipo de software malicioso projetado para fornecer ao invasor controle sobre o sistema da vítima. Os RATs são particularmente insidiosos porque permitem acesso remoto não autorizado, permitindo que invasores realizem diversas atividades maliciosas de forma discreta. Os principais recursos e capacidades do malware RAT incluem:

- **Controle remoto**: Os RATs permitem que invasores controlem remotamente um sistema como se tivessem acesso físico a ele.
- **Operação secreta**: Geralmente operam ocultos em segundo plano, evitando a detecção pelos usuários e software de segurança.
- **Vigilância**: Alguns RATs podem capturar teclas digitadas (keyloggers), fazer capturas de tela ou ativar câmeras e microfones para fins de espionagem.
- **Manipulação do sistema**: Os invasores podem modificar as configurações do sistema, instalar malware adicional ou até mesmo excluir ou criptografar arquivos.

Os RATs representam uma ameaça significativa à segurança cibernética individual e organizacional. Sua capacidade de fornecer aos

invasores amplo controle sobre os sistemas infectados os torna uma ferramenta preferida para espionagem, roubo de dados e sabotagem.

Ransomware

Software malicioso projetado para bloquear o acesso a um sistema ou dados de computador, geralmente criptografando arquivos, até que uma quantia em dinheiro seja paga. Esta forma de malware tem como alvo indivíduos, pequenas e médias empresas, corporações e instituições governamentais. Abaixo estão suas principais características:

- **Criptografia de dados**: O ransomware criptografa os arquivos da vítima, tornando-os inacessíveis sem uma chave de descriptografia.
- **Demanda de resgate**: Normalmente, as vítimas são obrigadas a pagar um resgate, geralmente em criptomoedas como Bitcoin, para receber a chave de descriptografia.
- **Limite de tempo**: Muitas variantes de ransomware incluem uma contagem regressiva, ameaçando excluir a chave de descriptografia ou aumentar o valor do resgate se não for pago dentro do prazo definido.
- **Vetores de ataque**: Métodos de infecção comuns incluem e-mails de phishing, exploração de vulnerabilidades em software ou visitas a sites comprometidos.
- **Alvo**: O ransomware pode atingir organizações grandes e pequenas, com muitas variantes projetadas especificamente para se infiltrar em redes corporativas.
- **Exfiltração de dados**: Ransomware avançado também pode roubar dados antes da criptografia, ameaçando vazamentos de dados se o resgate não for pago, uma tática conhecida como “dupla extorsão”.

Trojan

Um tipo de malware que engana os usuários sobre sua verdadeira intenção. Nomeados em homenagem à antiga história grega do enganoso cavalo de madeira que levou à queda da cidade de Tróia, os trojans normalmente se disfarçam de software legítimo e inofensivo para induzir os usuários a instalá-los.

Abaixo segue os principais aspectos do malware trojan:

- **Decepção**: Os cavalos de Tróia se apresentam como software útil, interessante ou necessário para motivar os usuários a baixá-los e instalá-los.
- **Funcionalidade maliciosa oculta**: embora pareçam benignos, os trojans executam ações maliciosas uma vez ativados. Essas ações podem variar amplamente, desde o roubo de dados até a instalação de outros malwares.
- **Entrega de outros malwares**: os trojans geralmente atuam como veículos de entrega de outros softwares maliciosos, incluindo ransomware e spyware.

Installer

O malware Installer é um tipo de software malicioso que se disfarça como um programa de instalação legítimo. Nesse sentido, é semelhante a um trojan. No entanto, ao contrário dos trojans, que podem se passar por qualquer tipo de software, esta categoria imita especificamente os instaladores.

Os usuários normalmente são induzidos a baixar e executar instaladores, pensando que estão obtendo um aplicativo genuíno. Uma vez executado, o malware pode realizar diversas ações, como:

- **Roubar informações confidenciais**
- **Instalação de malware adicional**
- **Fornecer acesso remoto ao sistema infectado**

Keylogger

Software projetado para registrar secretamente as teclas digitadas no dispositivo da vítima. Aqui está uma análise de suas características:

- **Funcionalidade**: Keyloggers capturam cada pressionamento de tecla, incluindo senhas, mensagens e outros dados confidenciais.
- **Exfiltração de dados**: As teclas digitadas gravadas são normalmente enviadas para um servidor controlado pelo invasor.
- F**inalidade**: Usado para espionagem, roubo de identidade, sabotagem corporativa ou obtenção de acesso não autorizado.

- **Tipos**: Keyloggers baseados em software são os mais comuns, mas existem variantes de hardware, geralmente como dispositivos USB ou acessórios de teclado.
- **Distribuição**: Propagação por meio de phishing, downloads maliciosos ou como parte de um ataque multicomponente.

3 Conclusão

Malwares representam uma séria ameaça para organizações, capazes de causar danos extensos e variados. Eles podem se infiltrar silenciosamente nos sistemas, expondo dados confidenciais e comprometendo a integridade das informações. O impacto financeiro pode ser devastador, incluindo perda de receita, custos de recuperação e danos à reputação da empresa. Além disso, malwares podem reduzir a eficiência operacional, corrompendo processos e sistemas vitais. O risco de interrupções no serviço e a perda de confiança dos clientes são consequências diretas.

A segurança cibernética robusta é essencial para prevenir esses riscos, exigindo vigilância constante e atualizações regulares. Portanto, as organizações devem priorizar a proteção contra malwares para garantir a continuidade dos negócios e a segurança de dados.

4 RECOMENDAÇÕES

Abaixo são elencados pela ISH, medidas que poderão ser adotadas visando a mitigação da infecção dos referidos *malwares*, como por exemplo:

Educação e treinamento dos funcionários

- Uma das maiores vulnerabilidades para qualquer organização é o erro humano. Treine seus funcionários para reconhecer e evitar cliques em links ou anexos suspeitos em e-mails, mensagens instantâneas ou redes sociais.

Atualizações e patches de segurança

- Mantenha todos os sistemas operacionais, softwares e aplicativos atualizados. Os patches de segurança frequentemente corrigem vulnerabilidades que poderiam ser exploradas por malwares.

Antivírus e anti-malware

- Instale e mantenha soluções de antivírus e anti-malware atualizadas. Estas ferramentas são essenciais para detectar e remover malwares antes que eles causem danos.

Firewalls

- Utilize firewalls para controlar o tráfego de entrada e saída da rede da sua organização. Isso pode ajudar a prevenir o acesso não autorizado e limitar a propagação de malwares.

Gerenciamento de acesso

- Implemente políticas de controle de acesso rigorosas. Garanta que os funcionários tenham apenas o nível de acesso necessário para realizar suas tarefas.

Backup de dados

- Realize backups regulares de dados importantes. Em caso de um ataque de malware, como um ransomware, você terá cópias de segurança dos seus dados.

Monitoramento de rede e análise de comportamento

- Monitore sua rede continuamente para detectar atividades suspeitas. Ferramentas de análise de comportamento podem ajudar a identificar padrões anormais que podem indicar uma infecção por malware.

Resposta a incidentes

- Tenha um plano de resposta a incidentes de segurança cibernética. Isso deve incluir etapas para isolar sistemas infectados, erradicar o malware e recuperar dados.

Auditoria e testes de segurança

- Realize auditorias de segurança regulares e teste sua infraestrutura com simulações de ataque (como testes de penetração) para identificar e corrigir vulnerabilidades.

Segurança de e-mail

- Implemente soluções de segurança de e-mail para filtrar spams e mensagens maliciosas. Isso reduz a probabilidade de phishing e outras formas de ataques baseados em e-mail.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- [Any.run]

heimdall
security research
A DIVISION OF ISH