kaspersky

Relatório analítico

Caminhos de malware: Uma análise das localizações de infostealers em sistemas de arquivos infectados

Análise das localizações de infostealers em sistemas de arquivos

Introdução

Os malwares de roubo de dados ("infostealers" ou "stealers") continuam sendo uma das categorias de malware mais difundidas e em rápida evolução. Conforme o nome sugere, o objetivo principal deles é roubar senhas e outros dados confidenciais dos dispositivos dos usuários. As informações coletadas são enviadas aos servidores de comando e controle dos atacantes na forma de arquivos de log.

Um **arquivo de log** é um arquivo comprimido composto por arquivos que contêm dados roubados do dispositivo de um usuário. A maioria deles são arquivos de texto com credenciais de contas, configurações de cookies e metadados.

Mais de

5 milhões

de arquivos de log contendo informações sobre o caminho para arquivos maliciosos foram analisados pela solução Kaspersky Digital Footprint Intelligence em 2025.

Kaspersky Digital Footprint Intelligence

Além dos metadados coletados de estações de trabalho infectadas, alguns malwares de roubo de dados também armazenam informações sobre o caminho para o arquivo executável onde o malware estava escondido.

Nossa análise dos arquivos de log publicados apresenta o volume e a natureza das infecções dos dispositivos dos usuários, bem como a forma como eles foram infectados. O relatório examina:

- Os diretórios mais comuns nos quais o malware está localizado,
- As técnicas utilizadas para disfarçar malware como arquivos legítimos de sistema e de usuário,
- Os nomes comuns de arquivos executáveis maliciosos,
- Os relacionamentos entre nomes de arquivos, métodos de distribuição e famílias de infostealer específicas,
- Os cenários reais de infecções de usuários.

As descobertas e as conclusões do relatório são relevantes para todos os usuários de estações de trabalho modernas, desde leitores individuais até funcionários de grandes corporações, agências governamentais e pequenas e médias empresas.

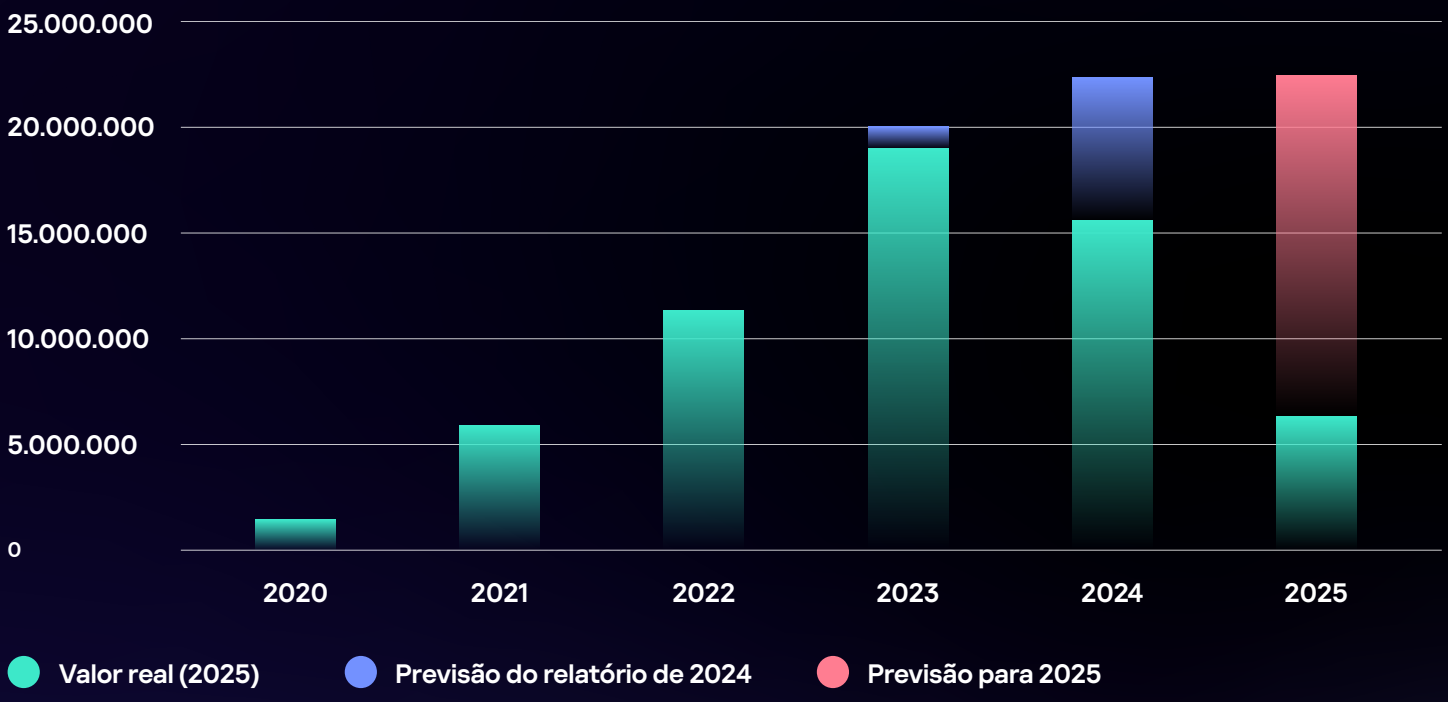
Essa é a terceira parte da nossa série sobre ameaças de infostealers. Acesse os links para ler a primeira e a segunda parte.

Estatísticas de infecções de usuários

Uma proporção significativa dos arquivos de log aparece na dark web após algum tempo: por exemplo, arquivos de log datados de 2024 começaram a ser publicados ao final daquele ano e em 2025. Espera-se que muitos arquivos de log datados de 2025 sejam publicados em 2026.

Como consequência, as estatísticas anuais de infecção podem ser revistas no futuro e as estatísticas para 2025 incluem valores projetados.

Estatísticas anuais de infecção, de 2020 a 2025 (observadas e projetadas)



Nosso relatório de 2024 fez as seguintes previsões de infecção:

- **2023 - 20 milhões de usuários,**
- **2024 - 22,5 milhões de usuários.**

O número real de infecções em 2023 foi de 19 milhões (um desvio de -4,61% em relação à previsão), e em 2024, o número foi de 15 milhões (um desvio de -30,80%). Quanto a 2025, nossa análise incluiu arquivos de log recém-descobertos datados de 2023, levando a um aumento de 11,46%. E em 2024, arquivos de log datados de 2022 foram incluídos na análise, o que resultou em um aumento de 4,48%.

Essa diferença numérica indica um aumento no período necessário para acumular dados completos. Considerando essa tendência, a previsão de infecção para 2024 permanece inalterada: aproximadamente 22,5 milhões de dispositivos de usuários.

A previsão de infecção para 2025 se assemelha à de 2024: de 20 a 25 milhões de dispositivos infectados (22,5 milhões em média).

Análise de metadados em registros de infostealers

Um dos parâmetros encontrados nos logs dos infostealers é o **caminho do malware**, ou seja, o caminho para o diretório que contém o arquivo executável do malware (o local exato onde ele foi instalado quando o dispositivo foi infectado), bem como o nome do arquivo.

A tabela abaixo mostra a frequência de caminhos específicos para diretórios em relação ao número total de registros de infostealers analisados em 2025.

Análise de caminhos para infostealers localizados em diretórios de usuários, em porcentagem (dados para 2025)

Caminho	%
C:\Users\<Usuário>\AppData\Local\Temp*	35,53%
C:\<Windows>\Microsoft.NET\Framework\<versão>*	32,33%
C:\Users\<Usuário>\AppData\Roaming*	8,40%
C:\Users\<Usuário>\Downloads*	6,60%
C:\Users\<Usuário>\Documents*	3,23%
C:\Users\<Usuário>\Desktop*	3,00%
Outros diretórios em C:\Users\<Usuário>\AppData\	2,56%
C:\<Windows>\Installer*	1,98%
C:\ProgramData*	1,77%
Outros diretórios em C:\Users\<Usuário>\	1,28%
C:\Users\<Usuário>\OneDrive*	0,71%
D:*	0,60%
C:\<Windows>\Temp*	0,56%
Outros diretórios na unidade C:\	0,50%
C:\Program Files**	0,40%
E:*	0,17%
Outra letra de unidade	0,16%
C:\Users\<Usuário>\Music*	0,12%
C:\Users\<Usuário>\Pictures*	0,10%
Recurso de rede compartilhado	0,01%

Como podemos ver, uma parte significativa de caminhos pertence aos diretórios **C:\Users\<Usuário>\AppData\Local\Temp*** e **C:\<Windows>\Microsoft.NET\Framework\<versão>***.

C:\Users\<Usuário>\AppData\Local\Temp é usado para armazenar arquivos temporários, incluindo dados temporários do navegador. Executar um arquivo executável por um navegador pode fazer com que ele seja salvo em **C:\Users\<Usuário>\AppData\Local\Temp**.

A presença de inúmeros registros que fazem referência a este diretório pode indicar que um malware está sendo executado sem antes ter sido salvo em um diretório específico.

Também analisamos os nomes de arquivos executáveis de infostealers no caminho do malware em **C:\<Windows>\Microsoft.NET\Framework\<versão>***.

Os 20 principais nomes de arquivos são os seguintes:

Nome do arquivo	Contagem
MSBuild.exe	661.638
RegAsm.exe	537.034
AppLaunch.exe	123.292
AddInProcess32.exe	50.724
[A-Za-z0-9]{10}\.exe	48.699
aspnet_regiis.exe	46.891
NETFXSBS10.exe	30.270
aspnet_compiler.exe	25.424
InstallUtil.exe	21.523
vbc.exe	20.886
aspnet_wp.exe	20.801
RegSvcs.exe	11.385
jsc.exe	7.814
ServiceModelReg.exe	6.077
csc.exe	6.050
System.dll	2.342
maxerste.exe	1.762
father121.exe	1.687
ilasm.exe	1.525
cvtres.exe	1.256

Aprenda mais sobre o malware de roubo de dados Lumma na Securelist.com

Note que um grande número de registros com o caminho **C:\<Windows>\Microsoft.NET\Framework\<versão>*** estão associadas ao mecanismo de malware que o injeta em um processo legítimo para burlar medidas de segurança. Essa técnica foi usada no malware de roubo de dados Lumma, por exemplo.

As campanhas do Lumma implementaram diversos métodos de distribuição. O mais notável foi a injeção de um payload na seção overlay de um freeware legítimo.

É intuitivo para o usuário salvar arquivos no diretório **C:\Users\<Usuário>\AppData\Local\Temp***, mas no caso do **C:\<Windows>\Microsoft.NET\Framework\<versão>**, trata-se de uma prova de um malware imitando componentes da Microsoft (cujos nomes correspondem a pacotes legítimos). Para obter estatísticas mais relevantes, excluímos da amostra duas categorias de caminhos principais: **(C:\Users\<Usuário>\AppData\Local\Temp*** e **C:\<Windows>\Microsoft.NET\Framework\<versão>*)** , e agrupamos as categorias com o menor número de registros.

Proporção de caminhos para infostealers localizados nos diretórios do usuário, exceto categorias excluídas, em porcentagem (dados de 2025)

Caminho	%
C:\Users\<Usuário>\AppData\Roaming*	26,12%
C:\Users\<Usuário>\Downloads*	20,53%
C:\Users\<Usuário>\Documents*	10,05%
C:\Users\<Usuário>\Desktop*	9,32%
Outros diretórios em C:\Users\<Usuário>\AppData\	7,97%
C:\<Windows>\Installer*	6,17%
C:\ProgramData*	5,50%
Outros diretórios em C:\Users\<Usuário>\	4,00%
C:\Users\<Usuário>\OneDrive*	2,22%
D:*	1,88%
C:\<Windows>\Temp*	1,74%
Outros diretórios na unidade C:\	1,55%
C:\Program Files**	1,23%
Outras	1,72%

Roaming contém principalmente arquivos relacionados a aplicativos, o que neste caso indica que um malware pode ter invadido uma estação de trabalho do usuário por meio de um aplicativo. A probabilidade de o usuário baixá-los de forma intencional é muito baixa. Portanto, os diretórios de usuários que mais nos interessam são **Downloads**, **Documentos** e **Área de trabalho**, pois estes costumam ser os locais em que um malware disfarçado de arquivos inofensivos é salvo após ser baixado.

Alguns exemplos de caminhos completos para esses diretórios encontrados com maior frequência, com base nos arquivos de log analisados, podem ser visualizados no apêndice do relatório.

Comparação dos 20 nomes de arquivos executáveis mais comuns para esses diretórios:

	Downloads	Documentos	Desktop
1	Bootstrapper.exe	[A-Za-z0-9_]{24}.exe	Bootstrapper.exe
2	Set-up.exe	PerfectouinVans.exe	Set-up.exe
3	Bootstapper.exe	Bootstrapper.exe	Licence_Version_Loader.exe
4	setup.exe	S?t_u? [U?D].exe	setup.exe
5	Licence_Version_Loader.exe	f75282f1.exe	Aura.exe
6	Aura.exe	identity_helper.exe	Kiddion's Modest Menu.exe
7	Kiddion's Modest Menu.exe	Xeno.exe	Kiddion's Modest Menu v1.0.0.exe
8	IDPнь_PђCЃtivP°tPsr.exe	BootstrapperUI.exe	Loader.exe
9	Loader.exe	S?t_u? [U?D!].exe	IDPнь_PђCЃtivP°tPsr.exe
10	Kiddion's Modest Menu v1.0.0.exe	BootstrapperAppxx.exe	Bootstapper.exe
11	Kiddions Mod.exe	Set-up.exe	S?t_u? [U?D].exe
12	Adobe_Activator.exe	setup.exe	Collapse.exe
13	activate.exe	XenoBootstrapper.exe	Adobe_Activator.exe
14	Xeno.exe	XenoIU.exe	activate.exe
15	identity_helper.exe	BootstrapperLua.exe	Xeno.exe
16	AdPsbe_Activator.exe	Xeno Release.exe	Kiddions Mod.exe
17	Verus.exe	XenoB.exe	modest-menu.exe
18	S?t_u? [U?D].exe	Licence_Version_Loader.exe	FusionLoader v2.1.exe
19	FusionLoader v2.1.exe	c06cdda6.exe	Verus.exe
20	BootstrapperUI.exe	kosdko0.exe	S?t_u? [U?D!].exe

Alguns nomes de arquivos parecem ser gerados usando uma máscara de arquivo específica, o que significa que o nome não é fixo ou exclusivo, mas pode variar de acordo com uma lógica definida. Por exemplo, os diretórios **SimpleAdobe**, **GuardFox** e **piratemamm** podem conter um arquivo que corresponde à máscara **[A-Za-z0-9_]{24}.exe**. Exemplos:

- C:\Users\<Usuário>\Documents\SimpleAdobe\GpQC1mCb9qtDeLNO_B1Ar08_.exe
- C:\Users\<Usuário>\Documents\SimpleAdobe\TL5EtTgS7O_di1ACG4eQaHrl.exe
- C:\Users\<Usuário>\Documents\GuardFox\Pm68igyBd5rQoMnsyLCAygRl.exe
- C:\Users\<Usuário>\Documents\piratemamm\hRAssuW6MEXEJiniYHLzXZ1l.exe

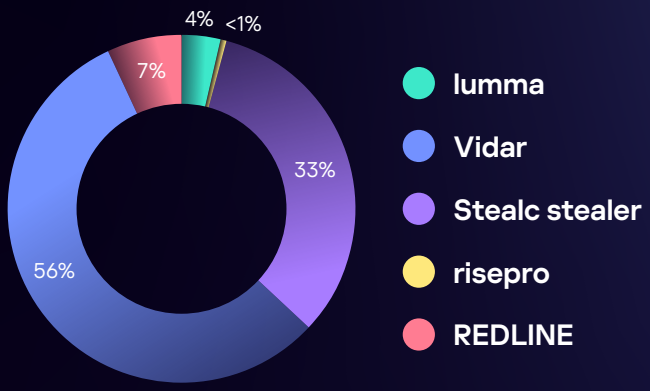
Outros nomes parecem mais significativos. Como podemos ver, é muito comum que o nome de um arquivo de malware corresponda a um arquivo de instalação **(Bootstapper.exe**, **Set-up.exe**, **setup.exe)** ou a um ativador **(Adobe_Activator.exe**, **activate.exe)**, ou seja, programas usados para a ativação ilegal de softwares ou de sistemas operacionais. Esses programas tendem a ser distribuídos por sites não confiáveis e lojas de aplicativos não oficiais.

Instalar software de fontes não confiáveis e tentar ativá-lo ilegalmente estão entre as principais causas de infecção do sistema do usuário.

Estatísticas por tipo de malware de roubo de dados para os nomes de arquivos de malware mais comuns localizados nos diretórios Downloads, Documentos e Área de trabalho:

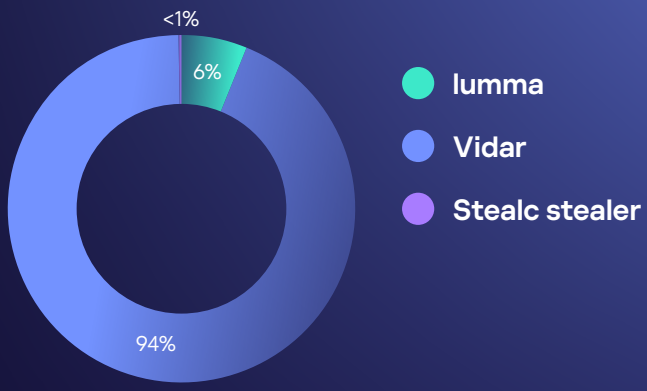
Conforme mostra o gráfico, os nomes que correspondem à máscara **[A-Za-z0-9_]{24}.exe** foram encontrados com maior frequência nos caminhos de malware dos malwares de roubo de dados **RisePro** e **Stealc**.

[A-Za-z0-9_]{24}.exe



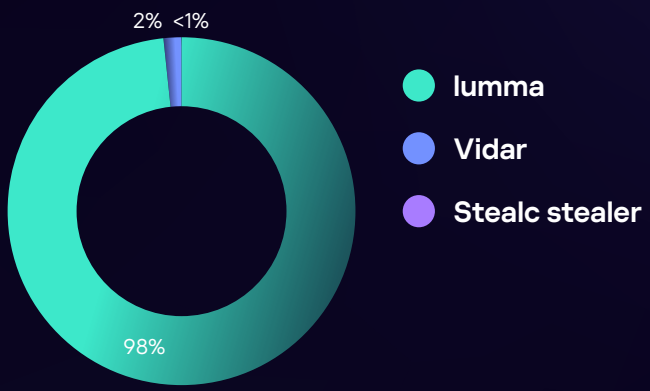
O nome **Bootstapper.exe** aparece com mais frequência em arquivos de log dos malwares de roubo de dados **Vidar** e **Lumma**.

Bootstrapper.exe



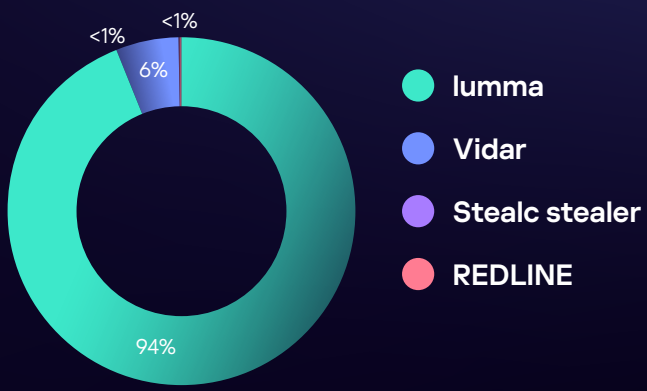
O nome **Set-up.exe** aparece com mais frequência em arquivos de log do malware de roubo de dados **Lumma**.

Set-up.exe



O nome **setup.exe** aparece com mais frequência em arquivos de logs do malware de roubo de dados **Lumma**, com uma pequena porcentagem encontrada nos arquivos do **Vidar**.

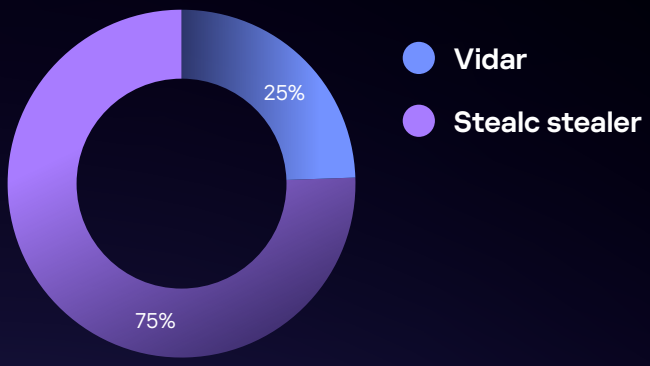
setup.exe



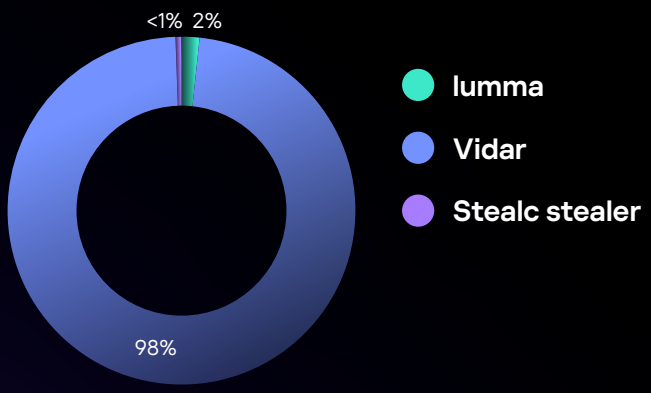
Conforme mostra o gráfico, o nome **Licence_Version_Loader.exe** aparece com mais frequência em arquivos de log dos malwares de roubo de dados **Stealc** e **Vidar**.

O nome **Bootstapper.exe** aparece com mais frequência em arquivos de log do malware de roubo de dados **Vidar**.

Licence_Version_Loader.exe



Bootstapper.exe



Note que o nome de um arquivo de malware depende mais do método de distribuição e das ações do atacante específico do que do tipo do malware de roubo de dados.

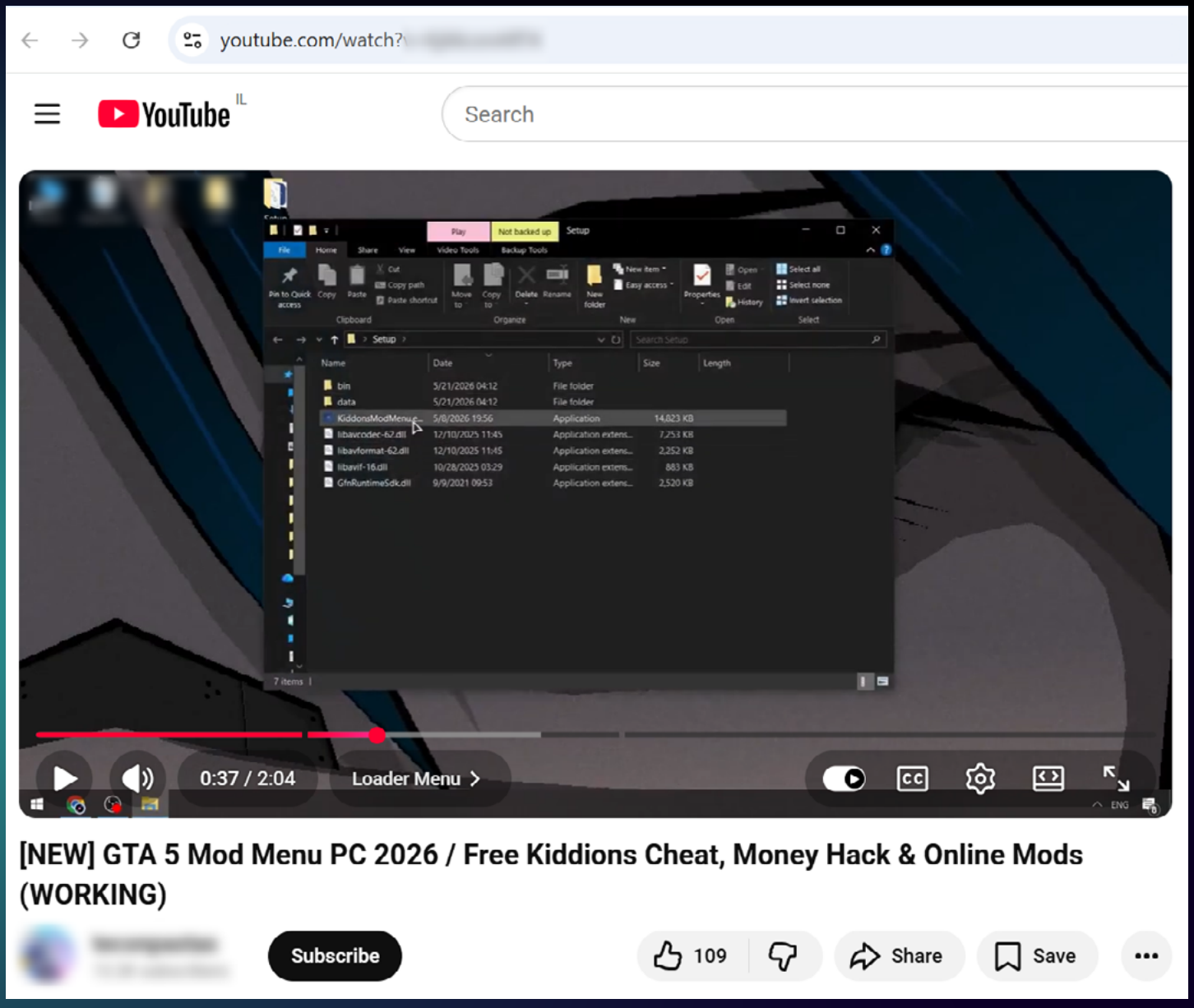
Além de arquivos de instalação e ativadores, é comum que malwares sejam distribuídos disfarçados de diversas modificações (mods) e complementos para jogos populares.

Por exemplo, o **Kiddion's Modest Menu** é um mod do Grand Theft Auto (GTA). Os usuários que procuram por esses mods de jogos on-line geralmente acabam virando vítimas de impostores de malware. Por exemplo, a palavra "kiddion" aparece em muitos dos nomes populares de arquivos executáveis listados acima.

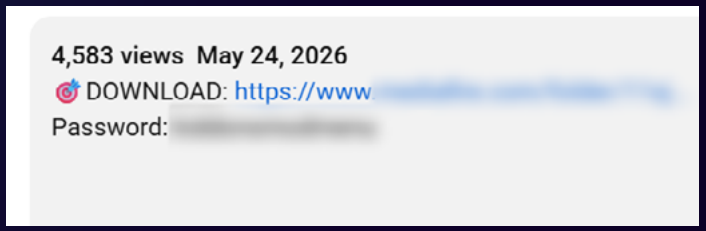
MPGPH131.exe, **MPGPH1.exe**, **MSIUpdaterV1.exe** e **MSIUpdaterV131.exe** são exemplos de nomes de arquivos executáveis geralmente associados ao malware de roubo de dados **RisePro**. Eles são responsáveis por 22% de todas as infecções do **RisePro**.

Exemplo de um golpe de distribuição de malware

A análise dos métodos de distribuição é um dos principais fatores para a detecção de malwares. Uma tática comum é persuadir os usuários a baixar e executar um arquivo executável. Para isso, os agentes de ameaças enviam vídeos a plataformas populares com instruções para instalar e executar softwares e complementos (como mods de jogos). Esses vídeos mostram um atacante executando o aplicativo e obtendo o resultado esperado.

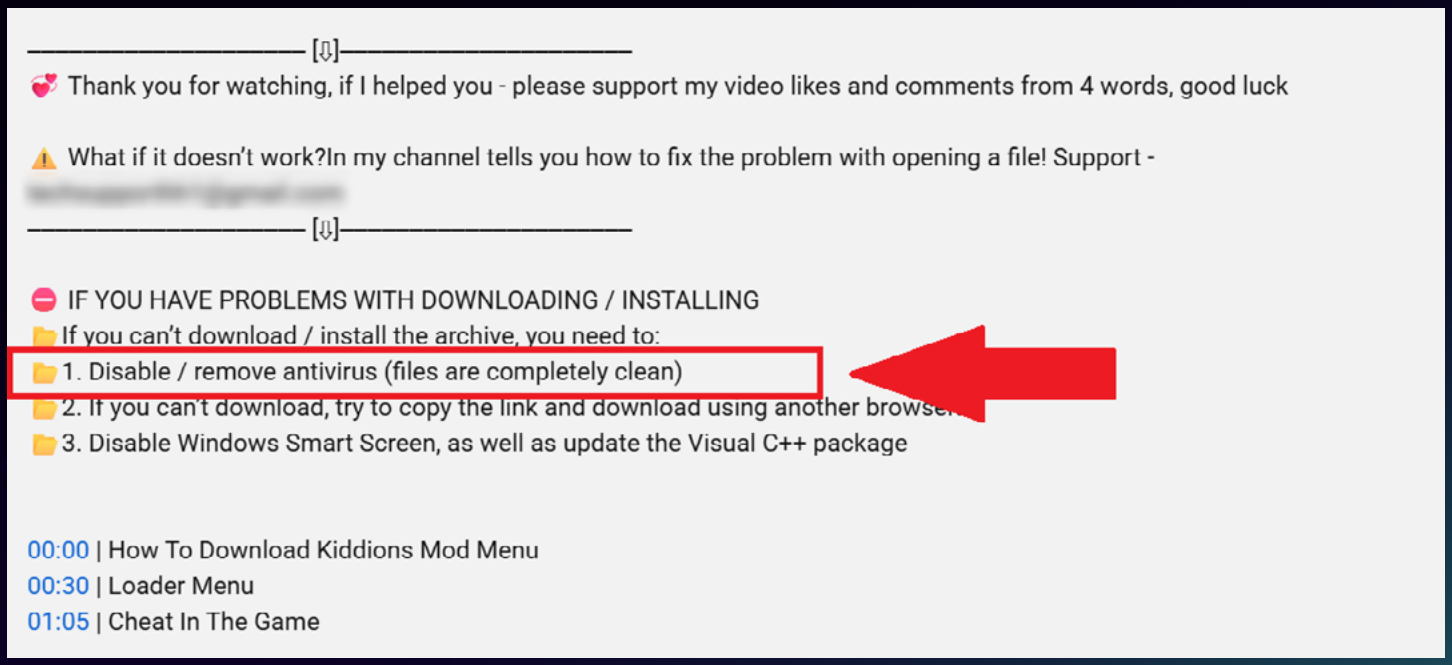


Então, um link para baixar o aplicativo é postado na seção de comentários. Você já deve ter percebido que o vídeo é falso e que o link de download contém um malware.



Via de regra:

- **O arquivo de download é um arquivo comprimido protegido por senha que contém um malware**
- **O usuário é instruído a desativar temporariamente todos os softwares de antivírus.**



Infelizmente, muitos usuários confiam na instrução e executam o arquivo malicioso. Note que o malware pode se disfarçar de quase todos os tipos de software, não apenas mods de jogos.

Conclusão

Nossa análise mostra que a distribuição dos infostealers é ampla e bastante padronizada, sendo que o comportamento do usuário, e não vulnerabilidades técnicas, representa o papel fundamental.

Uma proporção significativa dos caminhos encontrados em arquivos de log refere-se a softwares legítimos instalados na estação de trabalho de destino, o que reflete como esses softwares operam. Os malwares se infiltram em processos legítimos e contornam medidas de segurança.

Conclusão: os diretórios de usuários continuam sendo uma área de risco crítica.

A maior parcela de arquivos maliciosos é encontrada em dois tipos de diretórios:

- **C:\Users\<Usuário>\AppData\Local\Temp\ (cerca de 35%)**
  Esse caminho representa um cenário em que arquivos são executados diretamente pelo navegador sem que sejam salvos de forma explícita. Isso comprova que uma parcela significativa dos ataques não requer mascaramento complexo, pois os próprios usuários iniciam o processo.
- **C:\Windows\Microsoft.NET\Framework\ (cerca de 32%)**
  Esse caminho se assemelha a técnicas de injeção de processos e living-off-the-land, em que um malware se infiltra em processos legítimos. Esse comportamento é comum em famílias mais avançadas, como o Lumma.

A análise dos nomes dos arquivos revela um padrão de agrupamento claro:

1. Instaladores e carregadores que imitam a instalação de softwares legítimos:
   - setup.exe
   - Set-up.exe
   - Bootstrapper.exe
2. Ativadores e cracks que estão diretamente vinculados a softwares piratas e constituem um dos principais vetores de infecção:
   - Adobe_Activator.exe
   - activate.exe
   - Licence_Version_Loader.exe
3. Softwares que imitam mods de jogos e utilitários:
   - Kiddion's Modest Menu
   - FusionLoader

Embora o nome do arquivo seja determinado com mais frequência pelo cenário do ataque do que pelo próprio malware de roubo de dados, é possível encontrar padrões consistentes:

1. Lumma
   - setup.exe / Set-up.exe
   - Uso ativo de mascaramento de .NET
   - Injeção em processos legítimos
2. Vidar
   - Bootstrapper.exe
   - Bootstapper.exe
   - Carregadores clássicos
3. Stealc
   - Licence_Version_Loader.exe
   - Geração de nomes aleatórios
4. RisePro
   - MPGPH*.exe
   - MSIUpdater*.exe
   - Padrões de nomenclatura característicos e exclusivos (aproximadamente 22% dos casos)

Conclusão: o nome do arquivo é um indicador fraco, mas útil, especialmente quando se considera o caminho e o contexto.

O principal fator de infecções é o comportamento do usuário. Quase todos os cenários identificados podem ser associados a duas ações dos usuários: instalar softwares de fontes não confiáveis e tentar ativá-los ilegalmente. Infelizmente, os usuários costumam seguir as instruções dos agentes de ameaças e desativam o antivírus antes de executarem o arquivo malicioso.

As medidas tomadas para a prevenção dessas infecções devem ser abrangentes, além de incluírem o refinamento da lógica de detecção, o desenvolvimento de programas de conscientização e, é claro, a construção de um sistema de proteção baseado em cenários de usuários.

Proteja sua empresa contra ameaças ocultas

Kaspersky Digital Footprint Intelligence

Kaspersky Threat Intelligence

Nosso estudo sobre caminhos de arquivos de malware identificou que os locais de armazenamento de ameaças mais comuns são as pastas de download padrão, geralmente nativas no sistema. Além disso, esses programas tentam se disfarçar de processos legítimos para não serem detectados pelo usuário e pelos sistemas de segurança.

À medida que as informações e as tecnologias de rede evoluem, a higiene digital se torna cada vez mais importante para a proteção de usuários individuais e de empresas de todos os portes contra malwares distribuídos por arquivos baixados.

Kaspersky Digital Footprint Intelligence

Kaspersky Threat Intelligence

Anexo

Exemplos de caminhos completos para diretórios de usuários encontrados com maior frequência com base nos arquivos de log analisados:

- C:\Users\<Usuário>\Downloads\Kiddions Modest Menu\ Kiddion's Modest Menu\Kiddion's Modest Menu.exe
- C:\Users\<Usuário>\Downloads\Aura\Aura\Aura.exe
- C:\Users\<Usuário>\Downloads\LicPµnce.LPsadPµr(P A$$.- 2025)\Licence_Version_Loader.exe
- C:\Users\<Usuário>\Downloads\Kiddions Modest Menu v1.0.0\Kiddion's Modest Menu v1.0.0\Kiddion's Modest Menu v1.0.0.exe
- C:\Users\<Usuário>\Downloads\ui\Bootstapper.exe
- C:\Users\<Usuário>\Downloads\Kiddions_v2\Kiddions_v2\Kiddions Mod.exe
- C:\Users\<Usuário>\Downloads\Aura\Aura.exe
- C:\Users\<Usuário>\Downloads\FusionHacks\FusionHacks\FusionLoader v2.1.exe
- C:\Users\<Usuário>\Downloads\Adobe Photoshop\Adobe Photoshop\Set-up.exe
- C:\Users\<Usuário>\Documents\SimpleAdobe\[A-Za-z0-9_]{24}.exe
- C:\Users\<Usuário>\Documents\GuardFox\[A-Za-z0-9_]{24}.exe
- C:\Users\<Usuário>\Documents\piratemamm\[A-Za-z0-9_]{24}.exe
- C:\Users\<Usuário>\Documents\Perfectouin\Bin\PerfectouinVans.exe
- C:\Users\<Usuário>\Documents\iofolko5\[A-Za-z0-9_]{24}.exe
- C:\Users\<Usuário>\Documents\Minor Policy\[A-Za-z0-9_]{24}.exe
- C:\Users\<Usuário>\Documents\App\App\Bootstrapper.exe
- C:\Users\<Usuário>\Documents\UIBoot\UIBoot\BootstrapperUI.exe
- C:\Users\<Usuário>\Documents\Release\Release\XenoIU.exe
- C:\Users\<Usuário>\Desktop\Aura\Aura.exe
- C:\Users\<Usuário>\Desktop\Kiddion's Modest Menu\Kiddion's Modest Menu.exe
- C:\Users\<Usuário>\Desktop\Kiddion's Modest Menu v1.0.0\Kiddion's Modest Menu v1.0.0.exe
- C:\Users\<Usuário>\Desktop\Setup.exe
- C:\Users\<Usuário>\Desktop\Set-up.exe
- C:\Users\<Usuário>\Desktop\New folder\Licence_Version_Loader.exe
- C:\Users\<Usuário>\Desktop\Collapse\Collapse\Collapse.exe
- C:\Users\<Usuário>\Desktop\Adobe Photoshop\Set-up.exe
- C:\Users\<Usuário>\Desktop\Satu-p_32--64Bit\setup.exe
- C:\Users\<Usuário>\Desktop\UI\Bootstapper.exe
- C:\Users\<Usuário>\Desktop\Adobe Premiere Pro\Set-up.exe

Outros caminhos encontrados com frequência que podem ser úteis para fins de detecção:

- C:\Users\<Usuário>\1000029002\[a-f0-9]{10}.exe (например: C:\Users\<Usuário>\1000029002\9379a8d3cc.exe)
- C:\Users\<Usuário>\1000037002\[a-f0-9]{10}.exe
- C:\Users\<Usuário>\1000115002\[a-f0-9]{10}.exe
- C:\Users\<Usuário>\nM3kfb2gn5k.exe
- C:\Users\<Usuário>\PicoCo.exe
- C:\Users\<Usuário>\1000350002\[a-f0-9]{10}.exe
- C:\Users\<Usuário>\PlaneExplore.exe
- C:\Users\<Usuário>\11154530102\[a-f0-9]{10}.exe
- C:\Users\<Usuário>\Db94kfDkdls.exe
- C:\Users\<Usuário>\Bn5kgJsa2sf5n.exe

- C:\Windows\Installer\$PatchCache$\Managed\68AB67CA330133017706CB5110E47A00\21.1.20135_32bitmapibroker.exe
- C:\Windows\Installer\$PatchCache$\Managed\68AB67CA7DA73301B744BA0000000010\11.0.0\AcroRd32.exe
- C:\Windows\Installer\$PatchCache$\Managed\68AB67CA430133017706CB5110E47A00\21.1.20135_32bitmapibroker.exe
- C:\Windows\Installer\$PatchCache$\Managed\68AB67CA3301FFFF7706CB5110E47A00\21.1.20135_32bitmapibroker.exe
- C:\Windows\Installer\$PatchCache$\Managed\68AB67CA7DA73301B744CAF070E41400\15.7.20033\AcroRd32.exe
- C:\Windows\Installer\$PatchCache$\Managed\68AB67CA330100FF7706CB5110E47A00\21.1.20135_32bitmapibroker.exe
- C:\Windows\Installer\$PatchCache$\Managed\68AB67CA640133017706CB5110E47A00\21.1.20135_32bitmapibroker.exe
- C:\Windows\Installer\$PatchCache$\Managed\68AB67CA7DA73301B744CAF070E41400\15.7.20033\ADNotificationManager.exe
- C:\Windows\Installer\{307032B2-6AF2-46D7-B933-62438DEB2B9A}\ARPPRODUCTICON.exe
- C:\Windows\Installer\{4487064C-F31E-4499-A1EF-9B8E809A0358}\ARPPRODUCTICON.exe
- C:\Windows\Installer\{21DE6405-91DE-4A69-A8FB-483847F702C6}\ARPPRODUCTICON.exe
- C:\Windows\Installer\$PatchCache$\Managed\68AB67CA630133017706CB5110E47A00\21.1.20135_32bitmapibroker.exe
- C:\Windows\Installer\{42e5a8d4-8fb0-48a1-9063-fc159c7566a0}\ARPPRODUCTICON.exe
- C:\Windows\Installer\{18373B57-4FC3-4B1A-95B3-A7E5DCA577F7}\ARPPRODUCTICON.exe
- C:\Windows\Installer\{067039C9-A41C-42F5-9571-B06E0700AAA4}\icon.exe
- C:\Windows\Installer\{370C1839-B7D8-425E-8D3F-C79638E7D09C}\ARPPRODUCTICON.exe
- C:\Windows\Installer\{18469ED8-8C36-4CF7-BD43-0FC9B1931AF8}\ARPPRODUCTICON.exe
- C:\Windows\Installer\{06CD45E6-FF5E-4D8E-BC01-B276A90DADF2}\ARPPRODUCTICON.exe
- C:\Windows\Installer\$PatchCache$\Managed\68AB67CA3301FFFF7706C0F070E41400\15.7.20033\Acrobat_Elements.exe
- C:\Windows\Installer\{1E5C3247-B6FF-47F2-AEE9-A921B21E914F}\ARPPRODUCTICON.exe

- C:\Program Files (x86)\UltraStar Deluxe\songs\ultrastar deluxe songs pack
- C:\Program Files\Dassault Systemes\DraftSight\draftsight
- C:\Program Files (x86)\KONAMI\Pro Evolution Soccer 2013\crack pes
- C:\Program Files (x86)\VictorVal\Pro Evolution Soccer 2013 Repack\rld.dll pes
- C:\Program Files (x86)\Vital Office\Hasp\hardlock hasp hl emulator
- C:\Program Files (x86)\Sports Interactive\Football Manager 2005\fm
- C:\Program Files (x86)\Microsoft\EdgeUpdate\1.3.195.15\MicrosoftEdgeUpdateCore.exe
- C:\Program Files\Windows NT\[A-Za-z0-9]{43}.exe
- C:\Program Files\Lumion 4.5.1\Channels\lumion
- C:\Program Files\Google\Chrome\Application\updater.exe

- C:\Windows\Temp\Fb94JnkgmTbi.exe
- C:\Windows\Temp\[A-Za-z0-9]{13}.exe
- C:\Windows\Temp\[a-z0-9]{8}.[a-z0-9]{3}.exe
- C:\Windows\Temp\nM5Gkugn5b.exe
- C:\Windows\Temp\Gko5Kmko4n.exe

- C:\ProgramData\MPGPH131\MPGPH131.exe
- C:\ProgramData\MPGPH1\MPGPH1.exe
- C:\ProgramData\Lawai.com
- C:\ProgramData\MSIUpdaterV131_f09ac2d587354c6431bf93812ba7548f\MSIUpdaterV131.exe
- C:\ProgramData\MSIUpdaterV1\MSIUpdaterV1.exe
- C:\ProgramData\MSIUpdaterV1_b169c3872385b2c3c15a1f5f96f34ffe\MSIUpdaterV1.exe
- C:\ProgramData\MSIUpdaterV131_eeb341036f887f8bfa41fe84e80e9357\MSIUpdaterV131.exe
- C:\ProgramData\MSIUpdaterV131_c743bb12f321204aca6c69356124da3d\MSIUpdaterV131.exe
- C:\ProgramData\waf.com
- C:\ProgramData\Update\[A-Za-z0-9]{7}.exe

© 2026, AO Kaspersky Lab.
As marcas registradas e as marcas de serviço são a propriedade dos seus respectivos donos.