Análise de Códigos Maliciosos
Lumma Stealer

Artur Guimarães dos S. Leite[1], Marina S. Bon[1], Pedro B. Webber[1]

[1]Universidade do Vale do Rio dos Sinos (UNISINOS)
Porto Alegre – RS – Brasil

{leiteartur, bonmarina, webberpedro}@edu.unisinos.br

Resumo. *Este artigo descreve o comportamento do programa malicioso conhecido como Lumma Stealer através do uso de ferramentas que disponibilizam uma análise detalhada de suas comunicações. É importante ressaltar que a pesquisa foi feita com foco na área de Redes de Computadores e as ferramentas utilizadas foram para servir a tal propósito.*

1. Introdução

O *Lumma Stealer*, também denominado *LummaC2 Stealer*, é um programa malicioso, conhecido como malware, que ganhou fama nos últimos anos através de fóruns *Malware as a Service* (MaaS), locais que programadores disponibilizam seus códigos à venda para pessoas geralmente mal-intencionadas. Escrito em linguagem de programação C, incorporou uma técnica inovadora baseada em trigonometria. O *Lumma Stealer* espalha-se através de Cavalos de Tróia, ou seja, é incorporado à arquivos legítimos para enganar o usuário e, dessa forma, ser instalado no sistema de quem o acessa. Opera basicamente com operações web e é notável a existência de um servidor Comando e Controle (C&C), um local onde o atacante monitora e administra tanto as atividades do malware como as suas vítimas. Possui como principal alvo carteiras de criptomoedas.

Neste artigo, será discutido a respeito da funcionalidade do *Lumma Stealer*, com foco em suas comunicações envolvendo redes de computadores, as vulnerabilidades exploradas, as táticas, técnicas e procedimentos utilizados pelo malware e o roubo de credencias com extração de informações sensíveis da vítima.

2. Ambiente Configurado

Primeiramente, a fim de evitar a contaminação do computador pessoal e outros dispositivos conectados na rede, um ambiente virtual isolado foi configurado pela equipe de teste. Para isso, o aplicativo *Oracle VM* foi utilizado para rodar um sistema *Debian* que foi configurado em rede *NAT* para desassociá-lo da rede principal. Além disso, foi desativado qualquer tipo de área de transferência compartilhada, e foi usada uma função *Snapshot* que salva o estado do sistema no momento selecionado para possibilitar a recuperação em caso de infecção.

Além disso, utilizou-se um serviço on-line chamado Any Run em que é possível rodar amostras de arquivos e de URLs suspeitas em uma máquina virtual totalmente independente da rede pessoal para executar o teste do *Lumma Stealer*. O sistema operacional

escolhido foi o *Windows* 7 e a amostra foi adquirida no site *Malware Bazaar*, um projeto da abuse.ch para fortalecer a comunidade de segurança cibernética.

Figura 1. Detalhes da Máquina Debian

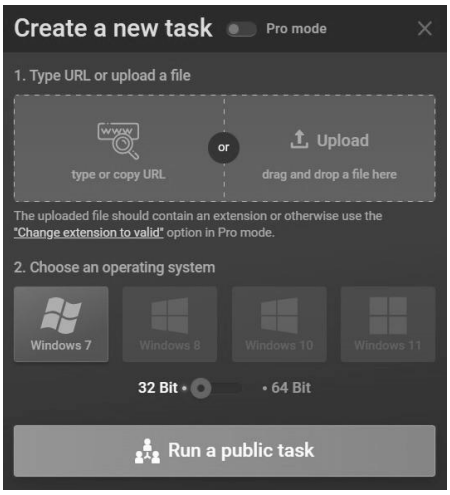


Figura 2. Detalhes da máquina Windows 7 no Any Run

3. Execução do malware

Com propósito de proteção da rede pessoal, a amostra do *Lumma Stealer* foi executada no site Any Run aberto em um sistema *Debian*, como já citado anteriormente. A amostra foi obtida na máquina com o *Debian* no site *Malware Bazaar* e transferida diretamente através de um arquivo *zip WinRAR* para o *Any Run*.

Após um curto período depois da execução do arquivo, o *Windows* 7 detectou a atividade maliciosa e reiniciou seu sistema operacional de forma automática. Em seguida, voltou à atividade em modo *Error Recovery*, apresentando quatro modos de

inicialização: *Safe Mode*, *Safe Mode with Networking*, *Safe Mode with Command Prompt* e Inicialização Normal. Os quatro modos foram testados para reinicialização e, após execução de ambos, o sistema apenas informou que um erro desconhecido foi encontrado, demonstrando que o *Lumma Stealer* passou desapercebido pelo sistema de segurança da máquina.

Figura 3. Pasta do arquivo contendo o *Lumma Stealer*

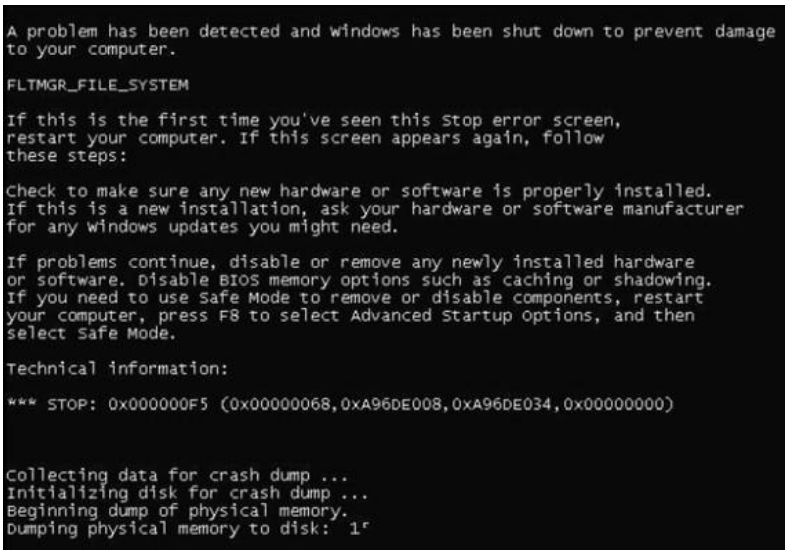


Figura 4. Mensagem de erro do *Windows* 7

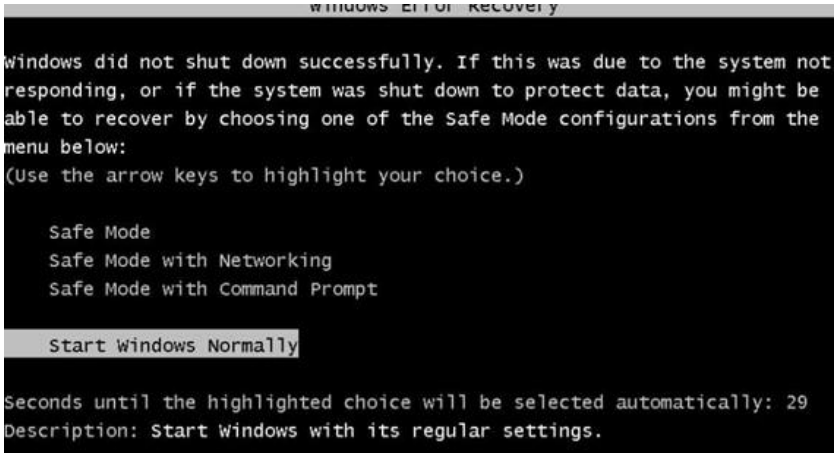


Figura 5. *Error Recovery* do *Windows* 7

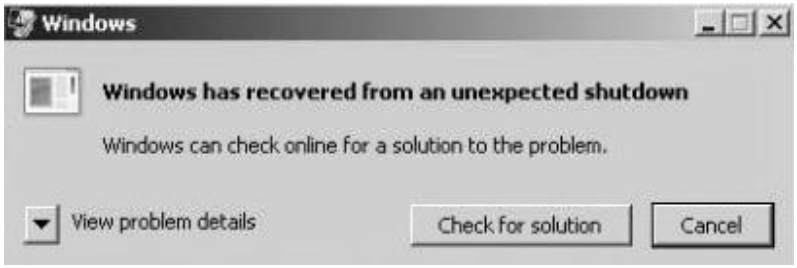


Figura 6. Mensagem após inicialização

4. Análises

Após o teste completo do malware, algumas informações foram obtidas com a ajuda de ferramentas. O site *Any Run* gerou um relatório com a atividade geral do malware durante o tempo de atividade na máquina, também disponibilizando um arquivo .pcap que é possível rodar no programa *Wireshark*, uma ferramenta capaz de capturar e de mostrar todos os pacotes gerados por uma máquina em seu funcionamento. Além disso, algumas ferramentas disponíveis abertamente na internet, conhecidas como *Open Source Intelligence* (OSINT), foram utilizadas para melhor entendimento da funcionalidade do *Lumma Stealer*.

4.1 Any Run

Com o relatório obtido no *Any Run* foi possível identificar a atividade e o caminho realizado pelo malware no sistema testado. Após a execução do arquivo, foram detectadas ações na pasta *Temp* do *Windows* 7, mostrando como foi possível o malware mascarar suas ações no sistema, pois os arquivos na pasta *Temp* são temporários e automaticamente apagados.

A pasta *framework* Microsoft.net também sofreu mudanças de acordo com o relatório. Nesta pasta foi detectado um arquivo executável desconhecido chamado AppLauncher.exe, realizando leituras e alterações nas *keys* registros de internet do *Windows*, o que pode significar uma tentativa de mudança de tráfego ou de violação dos protocolos de segurança.

O relatório apontou conexões *web* realizadas para o endereço IP 5.42.92.43, na qual foi possível detectar comunicações TCP e uma requisição HTTP POST, na qual é possível realizar extração de informações sensíveis. Portanto, é possível deduzir que o malware estava se comunicando com o servidor C&C através da web.

Timeshift	Class	PID	Process name
21368 ms	A Network Trojan was detected	2856	AppLaunch.exe
21377 ms	A Network Trojan was detected	2856	AppLaunch.exe
21379 ms	Potentially Bad Traffic	2856	AppLaunch.exe

Figura 7. Detecção do AppLaunch.exe pelo Any Run

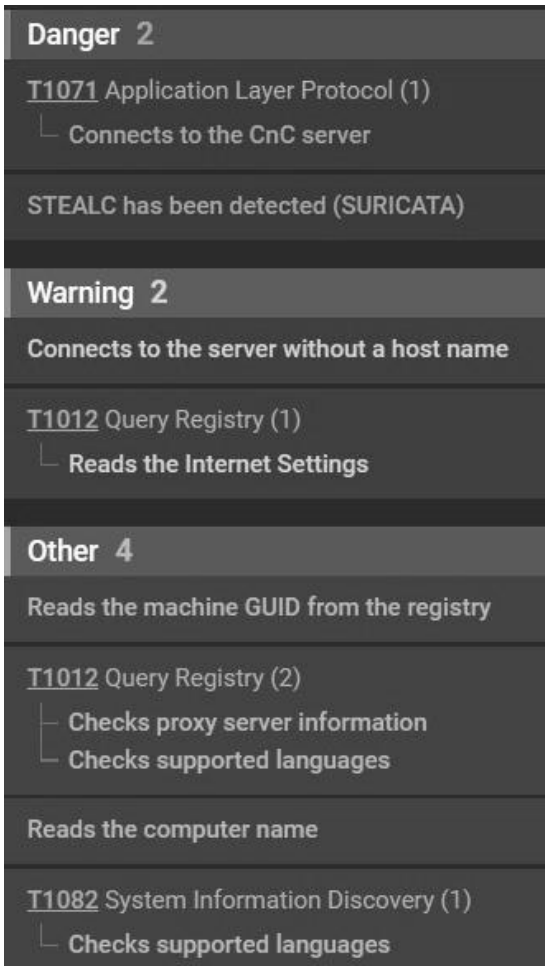


Figura 8. Processos maliciosos detectados pelo *Any Run*

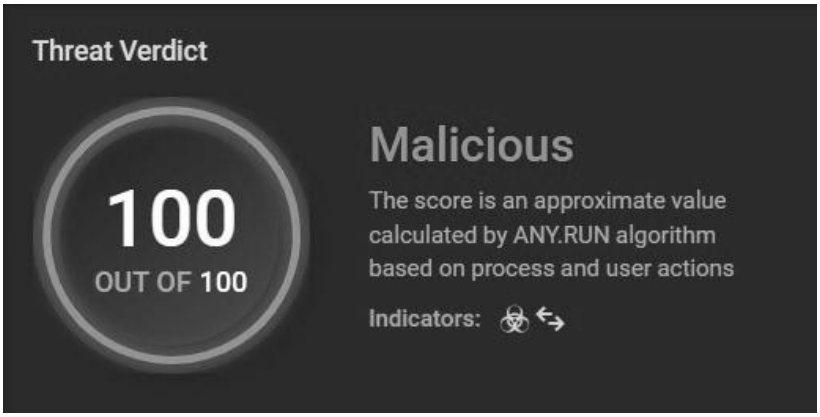
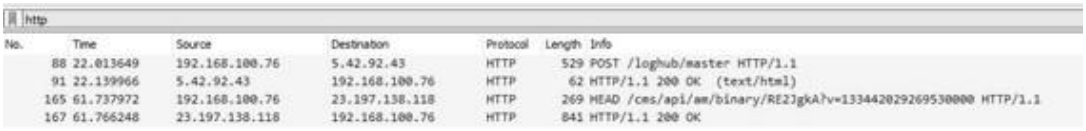


Figura 9. Veredito de ameaça pelo *Any Run*

4.2 *Wireshark*

Com o arquivo .pcap obtido pelo *Any Run*, é possível usar o aplicativo *Wireshark* para estudar os pacotes emitidos pela máquina. Filtrando os pacotes pelo IP do C&C, podemos ter uma visão mais detalhada da comunicação do *Lumma Stealer*. Como previsto, a troca de informações foi realizada basicamente pela web com requisições HTTP POST.



http

No.	Time	Source	Destination	Protocol	Length	Info
88	22.013649	192.168.100.76	5.42.92.43	HTTP	529	POST /loghub/master HTTP/1.1
91	22.139966	5.42.92.43	192.168.100.76	HTTP	62	HTTP/1.1 200 OK (text/html)
165	61.737972	192.168.100.76	23.197.138.118	HTTP	269	HEAD /cms/api/am/binary/RE2JgkA?v=133442029269530000 HTTP/1.1
167	61.766248	23.197.138.118	192.168.100.76	HTTP	841	HTTP/1.1 200 OK

Figura 10. Pacotes de comunicação com C&C

```
POST /loghub/master HTTP/1.1
Content-Type: multipart/form-data; boundary=HUGn9QVMTfdeR3MtLq9p
Content-Length: 213
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; InfoPath.1)
Host: 5.42.92.43
Connection: Keep-Alive
Cache-Control: no-cache

--HUGn9QVMTfdeR3MtLq9p
Content-Disposition: form-data; name="hwid"

MzIxQUExRjlCMDI5MzExMjY2NzQ0Nw==
--HUGn9QVMTfdeR3MtLq9p
Content-Disposition: form-data; name="build"

bmFyZG8=
--HUGn9QVMTfdeR3MtLq9p--
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Sat, 11 Nov 2023 20:01:28 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 8
Connection: keep-alive
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Referrer-Policy: same-origin

Tk8NCg==
```

1 client pkt(s), 1 server pkt(s), 1 turn(s).

Figura 11. Detalhes do pacote de HTTP *REQUEST*

4.3 *MITRE ATT&CK*

O programa *MITRE ATT&CK* consiste em uma base de dados acerca de táticas, técnicas e procedimentos conhecidos por serem realizados em atividade criminosa. Ao separar e classificar as ações do *Lumma Stealer* com base nas informações disponibilizadas no *MITRE ATT&CK*, é possível ter uma visão esclarecida e simplificada sobre seu funcionamento, facilitando também o ganho de conhecimentos para evitar esse tipo de ameaça.

Tabela 1. Funcionamento do Lumma Stealer segundo dados do MITRE ATT&CK

TA0005: Defense Evasion	TA0007: Discovery	TA0011: Command and Control
T1036: Mascara suas ações para parecer um programa legítimo.	T1012: Interage com os registros do Windows para ganhar informações pertinentes sobre o sistema.	T1071: O programa conecta-se com o C&C através da camada de aplicação.
T1036.003: Renomeia processos para parecer um programa legítimo.	T1082: O programa tenta descobrir informações sobre o sistema.	

4.4 *Open Source Intelligence* (OSINT)

Na contemporaneidade, é possível encontrarmos inúmeras ferramentas disponíveis na internet de forma aberta ao público que são de grande utilidade em pesquisas como esta. Para completar nosso conhecimento acerca do *Lumma Stealer*, algumas dessas ferramentas foram consultadas, tais como as seguintes:

4.4.1 *Shodan*

Shodan é conhecido por ser a primeira ferramenta de pesquisa por dispositivos e sistemas conectados na *web*. Através dele, foi possível ter uma visão esclarecedora sobre o endereço do Comando e Controle. Foi encontrado hosted-by.yeezyhost.net como *hostname* e as portas 22 (OpenSSH) e 80 (Nginx) abertas

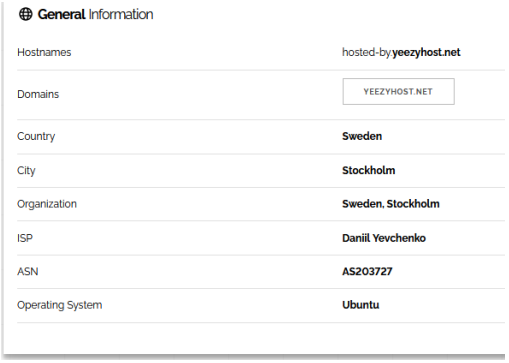


Figura 12. Detalhes do endereço no *Shodan*

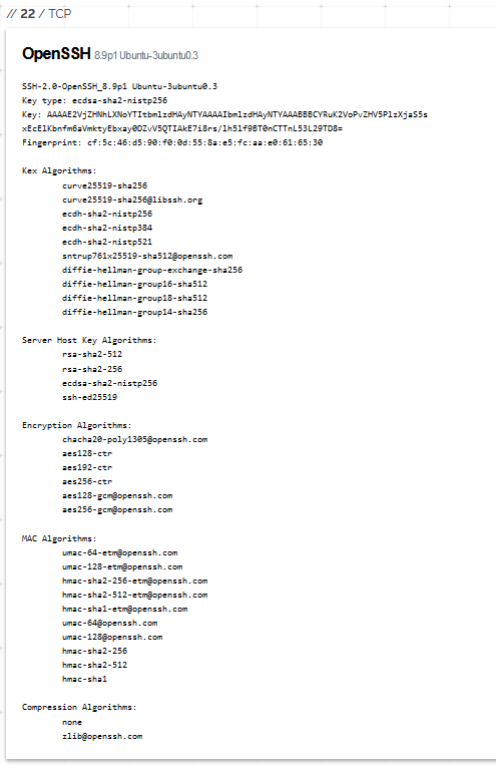


Figura 13. Análise do SSH pelo *Shodan*

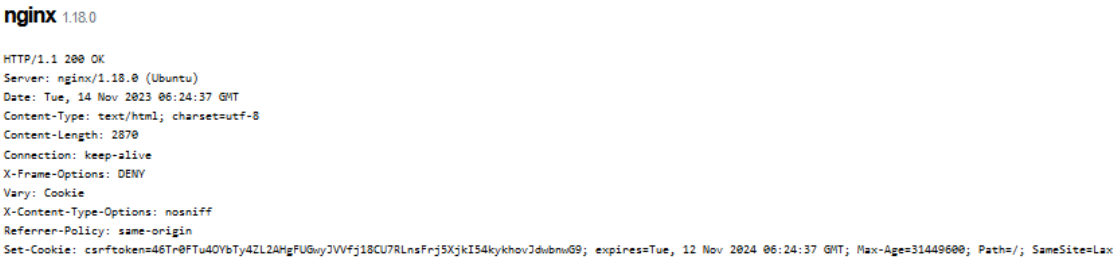


Figura 14. Análise da porta 80 pelo Shodan

4.4.2 *Cisco Talos Intelligence Group*

O *Cisco Talos Intelligence Group* é uma organização de inteligência em segurança cibernética. Na ferramenta foi observado que o IP estava em *blocklists* do spamhaus.org e da Cisco, como Cnc. Também é possível observar que o IP encontra-se ativo.

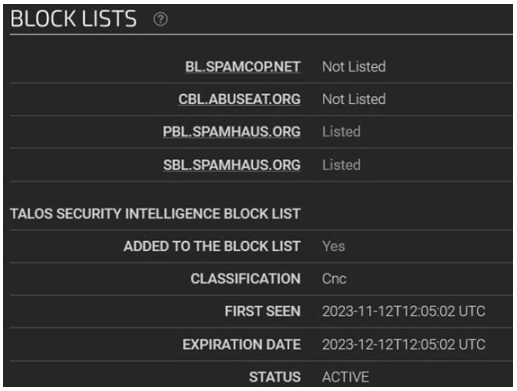


Figura 15. Relato de Blocklist pelo *Cisco Tallos*

4.4.3 *VirusTotal*

O *VirusTotal* é uma ferramenta que agrega diversos serviços de detecção de ameaças. Colocando o IP na ferramenta, vemos uma *flag*. A empresa ViriBack aponta esse IP como Cnc para o malware Mystic.

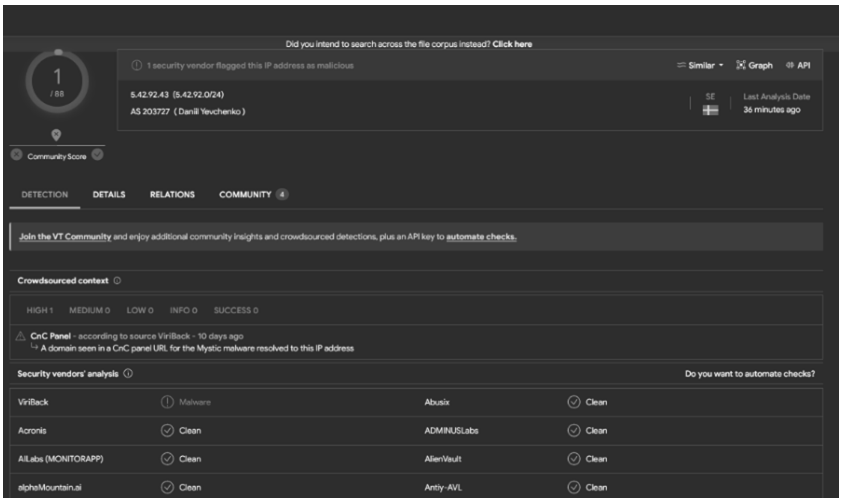


Figura 16. Análise do VirusTotal

4.4.4 *Open Threat Exchange AlienVault*

Open Threat Exchange é uma ferramenta da *AlienVault*, uma empresa de cibersegurança que fornece soluções contra ameaças virtuais, que permite o compartilhamento de informações sobre ameaças. Foi encontrada uma entrada com algumas informações sobre o *Lumma Stealer*. Nessa entrada são encontrados 216 indicadores de comprometimendo (IoCs) sendo, 4 IPs, 4 URLs e 3 Domínios além de *hashes* de arquivos. Na entrada também encontramos um gráfico do *VirusTotal* correlacionando arquivos, URLs e domínios.

Figura 17. Relato de atividade maliciosa pelo *Open Threar Exchange AlienVault*

Figura 18. Gráfico do *VirusTotal* encontrado

4.4.5 URLs encontradas

Durante a pesquisa foram encontradas duas URLs maliciosas relacionadas ao IP 5.42.92.43. A primeira delas foi encontrada no C2 *Tracker* da *ViriBack*.e a segunda nas investigações do *AlienVault*, indicando atividade recente do atacante e confirmando que o C&C continua ativo.

Malware	Url	IP	FirstSeen
Mystic	5.42.92.43/login	5.42.92.43	11-11-2023
Mystic	5.42.92.43/login/?next=/	5.42.92.43	11-11-2023

Figura 19. URLs encontradas no C2 *Tracker*

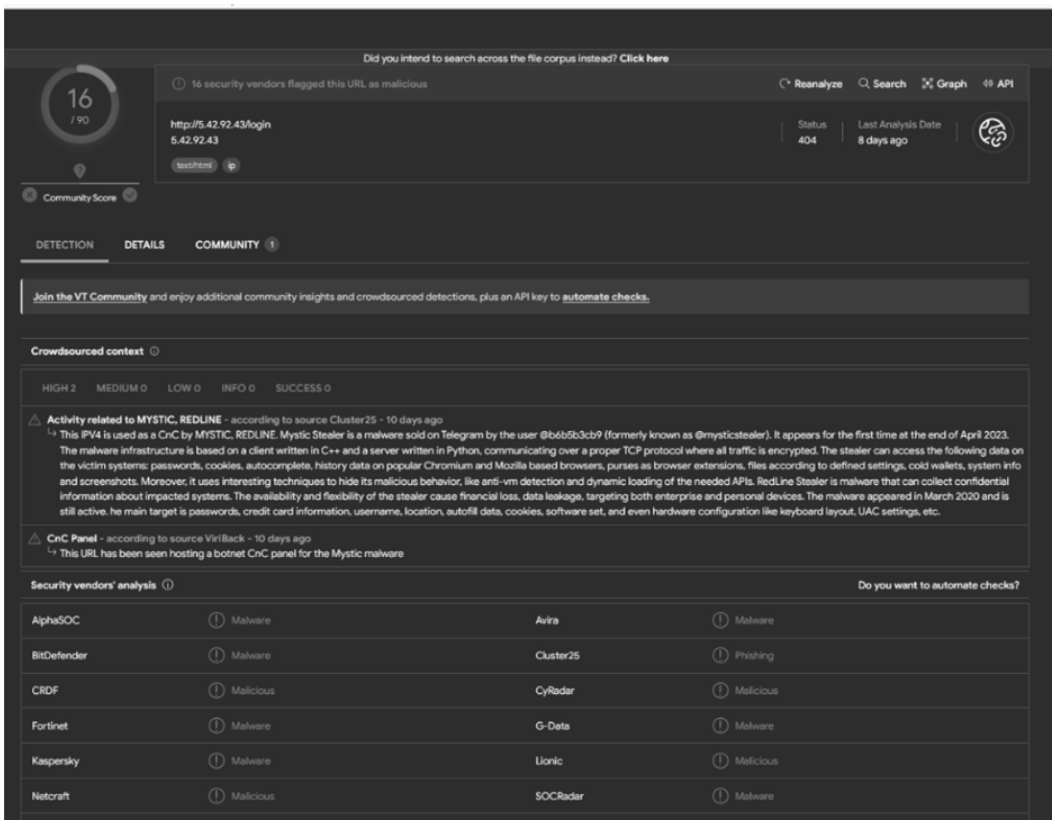


Figura 20. Análise de URLs *VirusTotal*

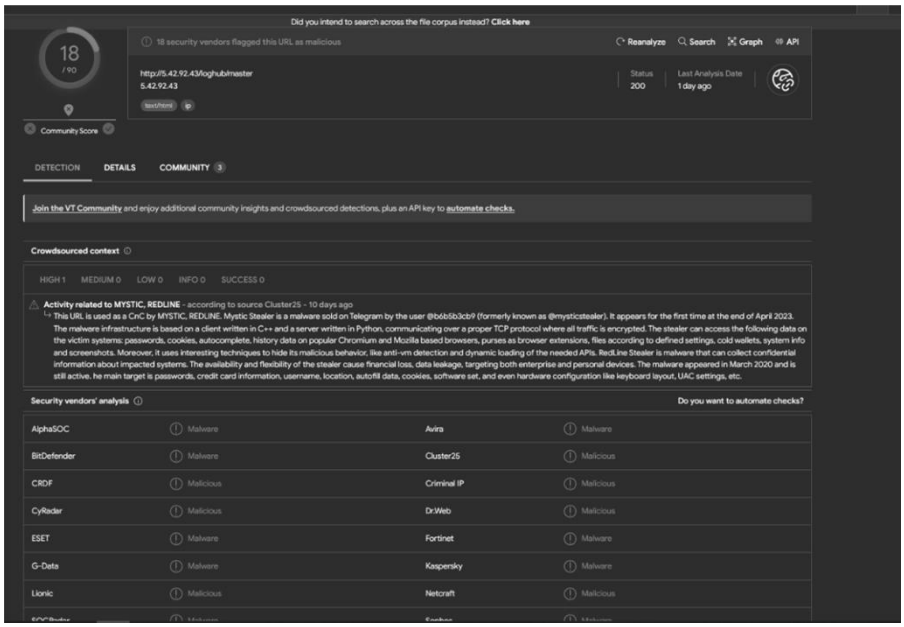


Figura 21. Análise de URLs *VirusTotal* 2

5. Conclusão

Em suma, o *Lumma Stealer* é um programa malicioso escrito em linguagem C e lógica trigonométrica. É disseminado através de Cavalos de Tróia, e ao infectar um computador utiliza protocolos web para extrair informações e comunicar-se com o C&C. Uma característica peculiar do *Lumma Stealer* é a possibilidade de mascarar seus rastros no sistema, operando através da pasta de arquivos temporários.

Nos tempos modernos, onde o uso da internet é cada vez mais rotineiro para o ser humano, se torna cada vez mais evidente a necessidade e importância de estarmos seguros on-line. Ameaças como a que foi estudada são, infelizmente, bastante comuns, e os criminosos têm noção da ignorância da população acerca da segurança cibernética. Por fim, vale ressaltar que estudos como este são cada vez mais indispensáveis, tendo em vista da crescente demanda por segurança em combate às crescentes ameaças cibernéticas.

Referências

Nedel, L. Bordini, R. Wagner, F. Hübner, J. “Instructions for Authors of SBC Conferences Papers and Abstracts”

Heimdall Security Research “Lumma Stealer”

Oracle VM https://www.virtualbox.org/

Any Run https://app.any.run/

Malware Bazaar https://bazaar.abuse.ch/

Shodan https://www.shodan.io/

VirusTotal https://www.virustotal.com/gui/home/upload

MITRE ATT&CK https://attack.mitre.org/

Malpedia “Lumma Stealer” https://malpedia.caad.fkie.fraunhofer.de/details/win.lumma

C2 Tracker https://tracker.viriback.com/

AlienVault AlienVault - Open Threat Exchange