



对手 ([HTTPS://WWW.SENTINELONE.COM/LABS/CATEGORY/ADVERSARY/](https://www.sentinelone.com/labs/category/adversary/))

从擦除器到勒索软件 | 阿格里乌斯的进化

阿米泰·本·蜀山·艾利希 ([HTTPS://WWW.SENTINELONE.COM/BLOG/AUTHOR/AMITAIB/](https://www.sentinelone.com/blog/author/amitaib/)) / 2021 年 5 月 25 日 ([HTTPS://WWW.SENTINELONE.COM/BLOG/2021/05/](https://www.sentinelone.com/blog/2021/05/))

执行摘要

- SentinelLabs 跟踪发现, Agrius 从 2020 年开始在以色列开展活动。
- Agrius 最初从事间谍活动, 对以色列目标部署了一系列破坏性擦除器攻击, 将该活动伪装成勒索软件攻击。
- 这些攻击是使用 *DEADWOOD* (又名 *Detbosit*) 进行的, 这是一个与伊朗威胁组织有未经证实的联系的擦除器。
- Agrius 演员还发布了一个名为“*Apostle*”的新型擦除器和一个名为“*IPsec Helper*”的自定义 .NET 后门。
- Agrius 后来进行的入侵表明, 他们不断维护和改进 *Apostle*, 将其变成了功能齐全的勒索软件。

活动。对乍一看似乎是勒索软件攻击的分析显示，在针对以色列目标的一系列破坏性攻击中部署了新的擦除器变体。攻击背后的操作者故意将其活动掩盖为勒索软件攻击。

攻击中使用的一个名为“*Apostle*”的擦拭器后来变成了功能齐全的勒索软件，取代了其擦拭器功能。里面的信息表明它被用来瞄准阿拉伯联合酋长国的一个重要的国有设施。与其擦拭版本的相似性，以及区域争端背景下目标的性质，使我们相信其背后的运营商正在利用勒索软件来实现其破坏能力。

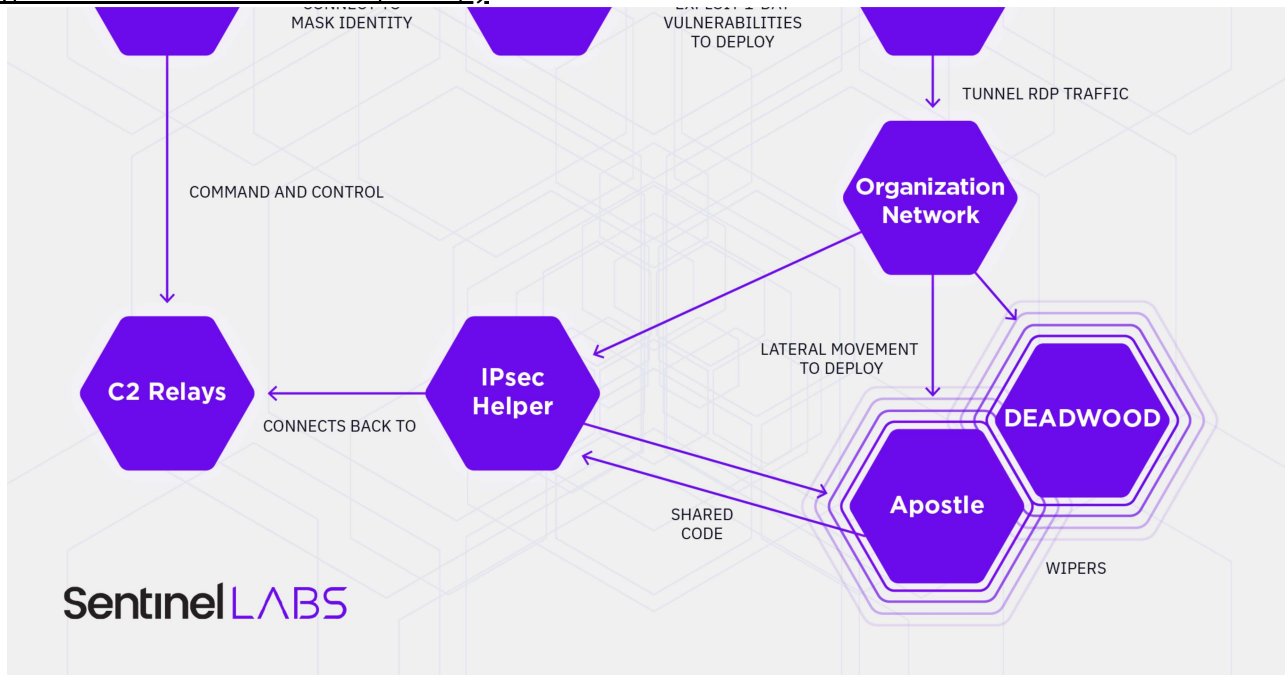
勒索软件作为破坏性工具的使用通常很难证明，因为很难确定威胁行为者的意图。对 *Apostle* 恶意软件的分析提供了对此类攻击的罕见洞察，在最初的擦除恶意软件和完全可操作的勒索软件之间划清了界限。

根据对工具和攻击基础设施的技术分析，我们中等信心地评估，这些攻击是由隶属于伊朗的威胁组织发起的。虽然观察到与已知伊朗行为者的一些联系，但 TTP 和工具集似乎是这组活动所独有的。SentinelLabs 追踪该威胁行为者为 Agrius。

Agrius 攻击生命周期

Agrius 威胁组织在访问其目标的面向公众的应用程序时，利用 VPN 服务（主要是 ProtonVPN）进行匿名化。成功利用后，威胁参与者会部署 Webshell 或仅使用目标组织的 VPN 解决方案访问目标。Agrius 部署的 webshell 大部分是 ASPXSpy (<https://attack.mitre.org/software/S0073/>) 的变体。

Agrius uses those webshells to tunnel RDP traffic in order to leverage compromised accounts to move laterally. During this phase, the attackers use a variety of publicly available offensive security tools for credential harvesting and lateral movement.



A summary of Agrius attack life cycle

On interesting hosts, the threat actor deploys its own custom malware – ‘*IPsec Helper*’. This backdoor is written in .NET and appears exclusive to Agrius. The malware registers itself as a service to achieve persistence. It can be used to exfiltrate data or deploy additional malware.

Agrius has deployed two different wipers. The first, dubbed ‘*Apostle*’, appears to be written by the same developer as ‘*IPsec Helper*’. Both are written in .NET, share functions, and execute tasks in a similar manner. Interestingly, *Apostle* was later modified into functioning ransomware. The second wiper, *DEADWOOD*, was previously involved in a wiping attack in the Middle East and tentatively attributed to Iran.

Attribution

Throughout our analysis of Agrius techniques, tools, and infrastructure, we found no solid links to any known threat groups. While it is hard to provide a definitive attribution for Agrius, a set of indications pointing the activity towards an Iranian nexus came up throughout the investigation:

1. Correlation with Iranian interests and past actions

While this is not a strong link, it is worth noting when correlated with other
<https://twitter.com/LabsSentinel>) [in](https://www.linkedin.com/company/sentinelone)(<https://www.linkedin.com/company/sentinelone>)

(<https://www.sentinelone.com/labs/>)

against Saudi Aramco. Since then, Iranian threat actors have been caught deploying wiper malware in correlation with the regime's interests on several occasions.

2. Webshells VirusTotal submissions

Some of the webshells deployed by Agrius throughout its intrusions were modified versions of ASPXSpy, deploying additional obfuscation and changing variable names. Three of the variants of this webshell were uploaded from Iran, the rest from other countries within the Middle East region.

While VirusTotal submissions are not an exact form of determining where a sample was deployed, the sources reinforce a Middle East regional focus.

Submissions ⓘ			
Date	Name	Source	Country
2020-08-10 07:30:04	c_base64.aspx	 c2d5de33 - web	IR


Submissions ⓘ			
Date	Name	Source	Country
2020-08-10 07:29:53	DBN_Base64.aspx	 c2d5de33 - web	IR


Modified Agrius webshells uploaded from Iran (source: VirusTotal

(<https://www.virustotal.com>))

3. Infrastructure links to Iran

The threat actor often used public VPN providers, such as ProtonVPN. On instances where the access was performed from non-VPN nodes, it originated from servers that have also resolved to Iranian domains in the past.

Q 54.37.99.4 ⓘ			
ASN	AS16276 - OVH	Netblock	54.37.0.0/16
Organization	OVH SAS		 FR
Resolve			
<input type="checkbox"/>	vip-panel.ir		
<input type="checkbox"/>	mail.samenferforgerobot.com		
<input type="checkbox"/>	mail.maralhosting.ir		
<input type="checkbox"/>	morghamingallery.ir		
<input type="checkbox"/>	dr.954a800878ba.farazhosting.ir		

Q 37.59.236.232 ⓘ			
ASN	AS16276 - OVH	Netblock	37.59.0.0/16
Organization	OVH SAS		 FR
Resolve			
<input type="checkbox"/>	avinakala.com		
<input type="checkbox"/>	soldaster.ir		
<input type="checkbox"/>	ns38.soldaster.ir		
<input type="checkbox"/>	ns37.soldaster.ir		

Agrius 使用了 DEADWOOD 雨刮器，该雨刮器此前被认为是由与伊朗有联系的演员所为。我们无法独立证实之前的聚类主张。Agrius 与最初部署 DEADWOOD 的威胁行为者之间的关系仍不清楚。这两个组可能有权访问共享资源。

结论

Agrius 是一个新的威胁组织，我们以中等信心评估其源自伊朗，从事间谍活动和破坏活动。该组织利用自己的定制工具集以及公开的攻击性安全工具来针对中东的各种组织。在某些情况下，该组织利用其访问权限来部署破坏性的擦除恶意软件，而在其他情况下则部署自定义勒索软件。考虑到这一点，我们发现 Agrius 不太可能是出于经济动机的威胁行为者。

我们对 Agrius 活动的分析并非凭空而来。2021 年 5 月初，伊朗发起了另一组针对以色列的破坏性勒索软件攻击，该攻击来自 n3tw0rm 勒索软件组织，该组织是一个新发现的威胁行为者，与 2020 年 (<https://www.bleepingcomputer.com/news/security/n3tw0rm-ransomware-emerges-in-wave-of-cyberattacks-in-israel/>) Pay2Key (<https://assets.sentinelone.com/labs/lessons-learned-from>) 攻击有关。Agrius 和 n3tw0rm 行动的密切距离表明它们可能是伊朗更大、协调的战略的一部分。Lab Dookhtegan 和 Project Signal (<https://www.flashpoint-intel.com/blog/second-iranian-ransomware-operation-project-signal-emerges/>) 勒索软件操作的泄密也支持了这一说法。

勒索软件活动虽然具有破坏性和有效性，但也提供了否认性，允许各国在不直接承担责任的情况下发出信息。其他民族国家资助的行为体也使用了类似的策略，产生了毁灭性的影响。其中最突出的是 2017 年的 NotPetya，这是一种针对乌克兰的破坏性恶意软件，伪装成勒索软件，并被西方情报机构归咎于 (<https://wccfttech.com/australia-us-uk-russia-notpetya/>) 俄罗斯国家支持的威胁行为者。

阅读完整报告

有关 IOC 的完整列表以及 Agrius 的更多详细信息，请参阅报告。

阅读完整报告 (<https://s1.ai/evol-agrius>)

(<https://www.sentinelone.com/labs/>)

雨刮器 ([HTTPS://WWW.SENTINELONE.COM/BLOG/TAG/WIPER/](https://www.sentinelone.com/blog/tag/wiper/))

分享

 Facebook

 Twitter

 LinkedIn

 Reddit

 Mail

PDF (<https://www.sentinelone.com/wp-content/uploads/pdf-gen/1630580702/from-wiper-to-ransomware-the-evolution-of-agrius.pdf>)



阿米泰·本·舒山·埃利希 (<https://www.sentinelone.com/blog/author/amitaib/>)

Amitai 是 SentinelOne 的威胁情报研究员，专门从事威胁情报、事件响应和威胁搜寻。在加入 SentinelOne 之前，他花了两年时间响应有针对性和出于经济动机的事件，重点关注威胁行为者的归因和特征分析。此前，他在 IDF 担任威胁研究员和威胁研究团队负责人超过 5 年。

上一篇

陷入云中 | 门罗币挖矿机如何利用 Docker 容器

(<https://www.sentinelone.com/labs/caught-in-the-cloud-how-a-monero-cryptominer-exploits-docker-containers/>)

下一个

贵族男爵 | 新的中毒安装程序可能被用于供应链攻击

(<https://www.sentinelone.com/labs/noblebaron-new-poisoned-installers-could-be-used-in-supply-chain-attacks/>)

(<https://www.sentinelone.com/labs/>)

加沙网络帮 | 统一战线针对哈马斯反对派
(<https://www.sentinelone.com/labs/gaza-cybergang-unified-front-targeting-hamas-opposition/>)

2023 年 12 月 14 日

网络软实力 | 中国大陆的收购
(<https://www.sentinelone.com/labs/cyber-soft-power-chinas-continental-takeover/>)

2023 年 9 月 21 日

中国纠缠 | 亚洲博彩业的 DLL 劫持
(<https://www.sentinelone.com/labs/chinese-entanglement-dll-hijacking-in-the-asian-gambling-sector/>)

2023 年 8 月 17 日

报名

当我们发布新内容时收到通知。

<https://twitter.com/LabsSentinel>) **in**(<https://www.linkedin.com/company/sentinelone>)

(<https://www.sentinelone.com/labs/>)

人数据。本网站受 reCAPTCHA 保护，并适用Google 隐私政策 (<https://policies.google.com/privacy>)和服务条款 (<https://policies.google.com/terms>)。

最近的帖子



(<https://www.sentinelone.com/labs/exploring-fbot-python-based-malware-targeting-cloud-and-payment-services/>)

探索 FBot | 针对云和支付服务的基于 Python 的恶意软件

(<https://www.sentinelone.com/labs/exploring-fbot-python-based-malware-targeting-cloud-and-payment-services/>)

2024 年 1 月 11 日



(<https://www.sentinelone.com/labs/labscon-replay-spectre-strikes-again-introducing-the-firmware-edition/>)

LABScon 重播 | 幽灵再次来袭：固件版本简介

(<https://www.sentinelone.com/labs/labscon-replay-spectre-strikes-again-introducing-the-firmware-edition/>)

2023 年 12 月 28 日



(<https://www.sentinelone.com/labs/labscon-replay-intellexa-and-cytrox-from-fixer-upper-to-intel-agency-grade-spyware/>)

LABSCon 重播 | Intellexa 和 Cytrox：从 Fixer-Upper 到英特尔代理级间谍软件

(<https://www.sentinelone.com/labs/labscon-replay-intellexa-and-cytrox-from-fixer-upper-to-intel-agency-grade-spyware/>)

2023 年 12 月 26 日

实验室类别

犯罪软件 (<https://www.sentinelone.com/labs/category/crimeware/>)

安全研究 (<https://www.sentinelone.com/labs/category/security-research/>)

高级持续威胁 (<https://www.sentinelone.com/labs/category/advanced-persistent-threat/>)

对手 (<https://www.sentinelone.com/labs/category/adversary/>)

实验室康 (<https://www.sentinelone.com/labs/category/labscon/>)

安全与情报 (<https://www.sentinelone.com/labs/category/security-intelligence/>)

哨兵实验室

在互联网时代，当市场、地域和司法管辖区融入数字领域的熔炉中时，威胁生态系统的危险变得无与伦比。犯罪软件家族的技术复杂程度达到了无与伦比的水平，APT 组织正在成熟的网络战中展开竞争，而曾经分散且分散的威胁行为者正在形成坚定的联盟，以精英企业间谍团队的身份运作。

最近的帖子



探索 FBot | 针对云和支付服务的基于 Python 的恶意软件
(<https://www.sentinelone.com/labs/exploring-fbot-python-based-malware-targeting-cloud-and-payment-services/>)

2024 年 1 月 11 日

(<https://www.sentinelone.com/labs/exploring-fbot-python-based-malware-targeting-cloud-and-payment-services/>)



LABScon 重播 | 幽灵再次来袭：固件版本简介
(<https://www.sentinelone.com/labs/labscon-replay-spectre-strikes-again-introducing-the-firmware-edition/>)

2023 年 12 月 28 日

(<https://www.sentinelone.com/labs/labscon-replay-spectre-strikes-again-introducing-the-firmware-edition/>)



LABSCon 重播 | Intellexa 和 Cytrox：从 Fixer-Upper 到英特尔代理级间谍软件
(<https://www.sentinelone.com/labs/labscon-replay-intellexa-and-cytrox-from-fixer-upper-to-intel-agency-grade-spyware/>)

(<https://www.sentinelone.com/labs/>).

from-fixer-
upper-to-
intel-agency-
grade-
spyware/)

报名

当我们发布新内容时收到通知。

企业邮箱



单击订阅即表示我同意根据 SentinelOne隐私政策 (/legal/privacy-policy/)使用我的个人数据。SentinelOne 不会向第三方出售、交易、出租或出借您的个人数据。本网站受 reCAPTCHA 保护，并适用Google 隐私政策 (<https://policies.google.com/privacy>)和服务条款 (<https://policies.google.com/terms>)。

推特

(<https://twitter.com/LabsSentinel>)

领英

(<https://www.linkedin.com/company/sentinelone>)

©2024 SentinelOne, 保留所有权利。