Tin tức an ninh mạng từ 16-03-2022 tới 23-03-2022

# Chinese 'Mustang Panda' Hackers Spotted Deploying New 'Hodur' Malware

📅Date: March 23, 2022 👤Author: Ravie Lakshmanan

Link tham khảo: *https://thehackernews.com/2022/03/chinese-mustang-panda-hackers-spotted.html*

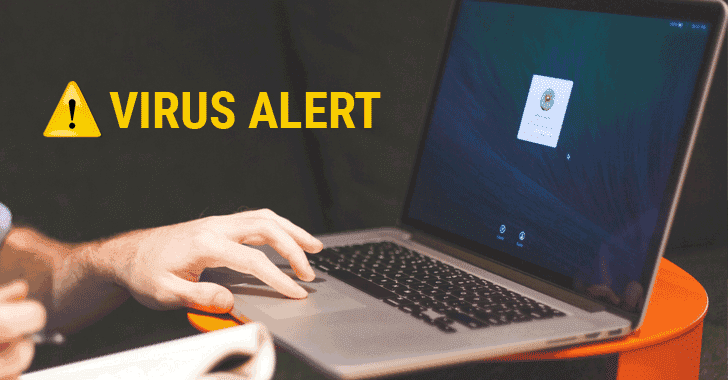


|  |  |
| --- | --- |
| Title: 🐄Chinese 'Mustang Panda' Hackers Spotted Deploying New 'Hodur' Malware | Title: 🐄Tin tặc 'Mustang Panda' Trung Quốc phát hiện triển khai phần mềm độc hại 'Hodur' mới |
| A China-based advanced persistent threat (APT) known as Mustang Panda has been linked to an ongoing cyberespionage campaign using a previously undocumented variant of the PlugX remote access trojan on infected machines. Slovak cybersecurity firm ESET dubbed the new version Hodur, owing to its resemblance to another PlugX (aka Korplug) variant called THOR that came to light in July 2021. "Most victims are located in East and Southeast Asia, but a few are in Europe (Greece, Cyprus, Russia) and Africa (South Africa, South Sudan)," ESET malware researcher Alexandre Côté Cyr said in a report shared with The Hacker News.  "Known victims include research entities, internet service providers (ISPs), and European diplomatic missions mostly located in East and Southeast Asia." Mustang Panda, also known as TA416, HoneyMyte, RedDelta, or PKPLUG, is a cyber espionage group that's primarily known for targeting non-governmental organizations with a specific focus on Mongolia. The latest campaign, which dates back to at least August 2021, makes use of a compromise chain featuring an ever-evolving stack of decoy documents pertaining to the ongoing events in Europe and the war in Ukraine.  "Other phishing lures mention updated COVID-19 travel restrictions, an approved regional aid map for Greece, and a Regulation of the European Parliament and of the Council," ESET said. "The final lure is a real document available on the European Council's website. This shows that the APT group behind this campaign is following current affairs and is able to successfully and swiftly react to them." Regardless of the phishing lure employed, the infections culminate in the deployment of the Hodur backdoor on the compromised Windows host.  "The variant used in this campaign bears many similarities to the THOR variant, which is why we have named it Hodur," explained. "The similarities include the use of the Software\CLASSES\ms-pu registry key, the same format for [command-and-control] servers in the configuration, and use of the Static window class." Hodur, for its part, is equipped to handle a variety of commands, enabling the implant to gather extensive system information, read and write arbitrary files, execute commands, and launch a remote cmd.exe session. The findings from ESET line up with public disclosures from Google's Threat Analysis Group (TAG) and Proofpoint, both of which detailed a Mustang Panda campaign to distribute an updated PlugX variant earlier this month. "The decoys used in this campaign show once more how quickly Mustang Panda is able to react to world events," Côté Cyr said. "This group also demonstrates an ability to iteratively improve its tools, including its signature use of trident downloaders to deploy Korplug."   Found this article interesting? Follow THN on Facebook, Twitter  and LinkedIn to read more exclusive content we post. | Một mối đe dọa dai dẳng nâng cao (APT) có trụ sở tại Trung Quốc được gọi là Mustang Panda có liên quan đến một chiến dịch gián điệp mạng đang diễn ra bằng cách sử dụng một biến thể không có tài liệu trước đây của trojan truy cập từ xa PlugX trên các máy bị nhiễm. Công ty an ninh mạng ESET của Slovakia đã đặt tên cho phiên bản mới là Hodur, do nó giống với một biến thể PlugX (hay còn gọi là Korplug) khác có tên là THOR được đưa ra ánh sáng vào tháng 7 năm 2021. Nhà nghiên cứu phần mềm độc hại của ESET, Alexandre Côté Cyr, cho biết trong một báo cáo được chia sẻ với The Hacker News: “Hầu hết nạn nhân ở Đông và Đông Nam Á, nhưng một số ít ở châu Âu (Hy Lạp, Síp, Nga) và châu Phi (Nam Phi, Nam Sudan). .  "Các nạn nhân được biết đến bao gồm các tổ chức nghiên cứu, các nhà cung cấp dịch vụ internet (ISP) và các cơ quan đại diện ngoại giao châu Âu hầu hết nằm ở Đông và Đông Nam Á." Mustang Panda, còn được gọi là TA416, HoneyMyte, RedDelta hoặc PKPLUG, là một nhóm gián điệp mạng chủ yếu được biết đến với việc nhắm mục tiêu vào các tổ chức phi chính phủ với trọng tâm cụ thể là Mông Cổ. Chiến dịch mới nhất, bắt đầu từ ít nhất là tháng 8 năm 2021, sử dụng một chuỗi thỏa hiệp bao gồm một chồng tài liệu mồi nhử ngày càng phát triển liên quan đến các sự kiện đang diễn ra ở châu Âu và cuộc chiến ở Ukraine.  "Các chiêu trò lừa đảo khác đề cập đến các hạn chế đi lại COVID-19 được cập nhật, bản đồ viện trợ khu vực đã được phê duyệt cho Hy Lạp và Quy định của Nghị viện Châu Âu và của Hội đồng", ESET cho biết. "Sự thu hút cuối cùng là một tài liệu thực có trên trang web của Hội đồng Châu Âu. Điều này cho thấy nhóm APT đằng sau chiến dịch này đang theo sát các vấn đề thời sự và có thể phản ứng thành công và nhanh chóng." Bất kể chiêu dụ lừa đảo được sử dụng, sự lây nhiễm lên đến đỉnh điểm trong việc triển khai cửa hậu Hodur trên máy chủ Windows bị xâm nhập.  "Biến thể được sử dụng trong chiến dịch này mang nhiều điểm tương đồng với biến thể THOR, đó là lý do tại sao chúng tôi đặt tên nó là Hodur," giải thích. "Những điểm tương đồng bao gồm việc sử dụng khóa đăng ký Software \ CLASSES \ ms-pu, cùng một định dạng cho máy chủ [command-and-control] trong cấu hình và sử dụng lớp cửa sổ tĩnh." Về phần mình, Hodur được trang bị để xử lý nhiều lệnh khác nhau, cho phép bộ cấy thu thập thông tin hệ thống rộng rãi, đọc và ghi các tệp tùy ý, thực thi lệnh và khởi chạy phiên cmd.exe từ xa. Các phát hiện từ ESET phù hợp với tiết lộ công khai từ Nhóm phân tích mối đe dọa của Google (TAG) và Proofpoint, cả hai đều nêu chi tiết chiến dịch Mustang Panda để phân phối biến thể PlugX cập nhật vào đầu tháng này. "Các mồi nhử được sử dụng trong chiến dịch này một lần nữa cho thấy Mustang Panda có thể phản ứng nhanh như thế nào với các sự kiện thế giới", Côté Cyr nói. "Nhóm này cũng thể hiện khả năng cải tiến lặp đi lặp lại các công cụ của mình, bao gồm cả việc sử dụng chữ ký của trình tải xuống đinh ba để triển khai Korplug."   Tìm thấy bài viết này thú vị? Theo dõi THN trên Facebook, Twitter  và LinkedIn để đọc thêm nội dung độc quyền mà chúng tôi đăng. |

# New Variant of Chinese Gimmick Malware Targeting macOS Users

📅Date: March 23, 2022 👤Author: Ravie Lakshmanan

Link tham khảo: *https://thehackernews.com/2022/03/new-variant-of-chinese-gimmick-malware.html*



|  |  |
| --- | --- |
| Title: 🐄New Variant of Chinese Gimmick Malware Targeting macOS Users | Title: 🐄Biến thể mới của phần mềm độc hại mánh lới quảng cáo của Trung Quốc Nhắm mục tiêu người dùng macOS |
| Researchers have disclosed details of a newly discovered macOS variant of a malware implant developed by a Chinese espionage threat actor known to strike attack organizations across Asia. Attributing the attacks to a group tracked as Storm Cloud, cybersecurity firm Volexity characterized the new malware, dubbed Gimmick, a "feature-rich, multi-platform malware family that uses public cloud hosting services (such as Google Drive) for command-and-control (C2) channels." The cybersecurity firm said it recovered the sample through memory analysis of a compromised MacBook Pro running macOS 11.6 (Big Sur) as part of an intrusion campaign that took place in late 2021.  "Storm Cloud is an advanced and versatile threat actor, adapting its tool set to match different operating systems used by its targets," Volexity researchers Damien Cash, Steven Adair, and Thomas Lancaster said in a report. "They make use of built-in operating system utilities, open-source tools, and custom malware implants to achieve their objectives. Leveraging cloud platforms for C2, such as using Google Drive, increases the likelihood of operating undetected by network monitoring solutions."  Unlike its Windows counterpart, which is coded in both .NET and Delphi, the macOS version is written in Objective C. The choice of the programming languages aside, the two versions of the malware are known to share the same C2 infrastructure and behavioral patterns. Once deployed, Gimmick is launched either as a daemon or in the form of a customized application that's engineered to impersonate a program frequently launched by the targeted user. The malware is configured to communicate with its Google Drive-based C2 server only on working days in order to further blend in with the network traffic in the target environment.  What's more, the backdoor, besides retrieving arbitrary files and executing commands from the C2 server, comes with its own uninstall functionality that allows it to erase itself from the compromised machine. To protect users against the malware, Apple has issued new signatures to its built-in anti-malware protection suite known as XProtect as of March 17, 2022 to block and remove the infections via its Malware Removal Tool (MRT). "The work involved in porting this malware and adapting its systems to a new operating system (macOS) is no light undertaking and suggests the threat actor behind it is well resourced, adept, and versatile," the researchers said.   Found this article interesting? Follow THN on Facebook, Twitter  and LinkedIn to read more exclusive content we post. | Các nhà nghiên cứu đã tiết lộ chi tiết về một biến thể macOS mới được phát hiện của một phần mềm độc hại được phát triển bởi một kẻ đe dọa gián điệp Trung Quốc được biết đến để tấn công các tổ chức tấn công trên khắp châu Á. Phân bổ các cuộc tấn công cho một nhóm được theo dõi là Storm Cloud, công ty an ninh mạng Volexity đã mô tả phần mềm độc hại mới, có tên Gimmick, một "họ phần mềm độc hại đa nền tảng, giàu tính năng sử dụng các dịch vụ lưu trữ đám mây công cộng (chẳng hạn như Google Drive) cho lệnh và- kênh điều khiển (C2). " Công ty an ninh mạng cho biết họ đã thu hồi mẫu thông qua phân tích bộ nhớ của một chiếc MacBook Pro bị xâm nhập chạy macOS 11.6 (Big Sur) như một phần của chiến dịch xâm nhập diễn ra vào cuối năm 2021.  "Storm Cloud là một tác nhân đe dọa tiên tiến và linh hoạt, điều chỉnh bộ công cụ của nó để phù hợp với các hệ điều hành khác nhau được các mục tiêu của nó sử dụng", các nhà nghiên cứu về Volexity Damien Cash, Steven Adair và Thomas Lancaster cho biết trong một báo cáo. "Họ sử dụng các tiện ích hệ điều hành tích hợp sẵn, công cụ mã nguồn mở và cấy ghép phần mềm độc hại tùy chỉnh để đạt được mục tiêu của mình. Việc tận dụng các nền tảng đám mây cho C2, chẳng hạn như sử dụng Google Drive, làm tăng khả năng hoạt động mà không bị phát hiện bởi các giải pháp giám sát mạng."  Không giống như phiên bản Windows, được mã hóa bằng cả .NET và Delphi, phiên bản macOS được viết bằng Objective C. Ngoài việc lựa chọn ngôn ngữ lập trình, hai phiên bản của phần mềm độc hại này được biết là có chung cơ sở hạ tầng C2 và các mẫu hành vi. Sau khi được triển khai, Gimmick được khởi chạy dưới dạng daemon hoặc ở dạng ứng dụng tùy chỉnh được thiết kế để mạo danh một chương trình được người dùng mục tiêu thường xuyên khởi chạy. Phần mềm độc hại được định cấu hình để giao tiếp với máy chủ C2 dựa trên Google Drive của nó chỉ vào những ngày làm việc nhằm hòa nhập sâu hơn với lưu lượng mạng trong môi trường mục tiêu.  Hơn nữa, backdoor, ngoài việc truy xuất các tệp tùy ý và thực hiện các lệnh từ máy chủ C2, còn có chức năng gỡ cài đặt riêng cho phép nó tự xóa khỏi máy bị xâm phạm. Để bảo vệ người dùng chống lại phần mềm độc hại, Apple đã ban hành chữ ký mới cho bộ bảo vệ chống phần mềm độc hại được tích hợp sẵn có tên là XProtect kể từ ngày 17 tháng 3 năm 2022 để chặn và loại bỏ các lây nhiễm thông qua Công cụ loại bỏ phần mềm độc hại (MRT). Các nhà nghiên cứu cho biết: “Công việc liên quan đến việc chuyển phần mềm độc hại này và điều chỉnh hệ thống của nó sang hệ điều hành mới (macOS) không hề nhẹ nhàng và cho thấy tác nhân gây ra mối đe dọa đằng sau nó có nguồn lực tốt, lão luyện và linh hoạt,” các nhà nghiên cứu cho biết.   Tìm thấy bài viết này thú vị? Theo dõi THN trên Facebook, Twitter  và LinkedIn để đọc thêm nội dung độc quyền mà chúng tôi đăng. |

# Use This Definitive RFP Template to Effectively Evaluate XDR solutions

📅Date: March 23, 2022 👤Author: The Hacker News

Link tham khảo: *https://thehackernews.com/2020/07/extended-detection-response.html*



|  |  |
| --- | --- |
| Title: 🐄Use This Definitive RFP Template to Effectively Evaluate XDR solutions | Title: 🐄Sử dụng Mẫu RFP Cuối cùng này để Đánh giá Hiệu quả các giải pháp XDR |
| A new class of security tools is emerging that promises to significantly improve the effectiveness and efficiency of threat detection and response.  Emerging Extended Detection and Response (XDR) solutions aim to aggregate and correlate telemetry from multiple detection controls and then synthesize response actions.  XDR has been referred to as the next step in the evolution of Endpoint Detection and Response (EDR) solutions.  Because XDR represents a new solution category, there is no single accepted definition of what capabilities and features should (and shouldn't) be included.  Each provider approaches XDR with different strengths and perspectives on how what an XDR solution should include.  Therefore, selecting an XDR provider is quite challenging as organizations must organize and prioritize a wide range of capabilities that can differ significantly between providers.  Cynet is now addressing this need with the Definitive RFP Template for XDR solutions (download here), an expert-made security requirement list that enables stakeholders to accelerate and optimize the evaluation process of the products they evaluate.  The RFP template aims to capture the widest common denominator in terms of security needs and deliver the essentials relevant to any organization.  An XDR solution can benefit large companies that are awash in alerts from multiple detection sources, rationalize the myriad signals, and simplify response actions. Smaller companies benefit by leveraging a single platform that would otherwise require coordinating several expensive and complex point solutions. Logically it makes sense for organizations to achieve greater threat visibility along with reduced complexity.  "Despite all the security tools that have been deployed over the years to prevent and detect breaches, attackers are still able to find the seams in the protections," says Eyal Gruner, CEO of Cynet. "One of the main problems is that security teams simply cannot make sense of the barrage of information and alerts coming at them from multiple security tools. And, some organizations can't afford to deploy all of the necessary monitoring tools to ensure full protection."  To provide strong breach protection, organizations must collect, synthesize, and make sense of signals from the primary attack vectors as the first step to better defense. Then, automating investigation and remediation to cover the full breadth of each attack ensures all appropriate actions are taken to protect the organization. This is where XDR comes in.  Using the ready-made templates can potentially save significant time and resources otherwise spent on building a similar requirement list from scratch. The XDR solution RFP can help companies prioritize the capabilities available in emerging solutions to improve their purchase decisions.  The RFP comprises five sections:   Monitoring & Control—routine activities to gain visibility and proactively discover and reduce attack surfaces. Prevention & Detection—mechanism to thwart the wide array of commodities and advanced attack vectors. Investigation & response—an overall toolset for efficient reaction to the detected live attacks. Infrastructure—architecture, deployment, data collection, and communication. Operation—ongoing management of the solution   The RFP Guides ensure organizations are not overlooking important aspects of security solution capabilities and thereby making substandard decisions for critical enterprise purchases.  Download the XDR RFP here.   Found this article interesting? Follow THN on Facebook, Twitter  and LinkedIn to read more exclusive content we post. | Một lớp công cụ bảo mật mới đang xuất hiện hứa hẹn sẽ cải thiện đáng kể hiệu lực và hiệu quả của việc phát hiện và ứng phó với mối đe dọa.  Các giải pháp Phản hồi và Phát hiện Mở rộng (XDR) mới nổi nhằm tổng hợp và tương quan giữa phép đo từ xa từ nhiều kiểm soát phát hiện và sau đó tổng hợp các hành động phản hồi.  XDR được coi là bước tiếp theo trong sự phát triển của các giải pháp Phát hiện và Phản hồi Điểm cuối (EDR).  Vì XDR đại diện cho một danh mục giải pháp mới, nên không có định nghĩa được chấp nhận duy nhất về những khả năng và tính năng nào nên (và không nên) được đưa vào.  Mỗi nhà cung cấp tiếp cận XDR với các điểm mạnh và quan điểm khác nhau về cách một giải pháp XDR nên bao gồm.  Do đó, việc lựa chọn một nhà cung cấp XDR là khá khó khăn vì các tổ chức phải tổ chức và ưu tiên một loạt các khả năng có thể khác nhau đáng kể giữa các nhà cung cấp.  Cynet hiện đang giải quyết nhu cầu này với Mẫu RFP cuối cùng cho các giải pháp XDR (tải xuống tại đây), một danh sách yêu cầu bảo mật do chuyên gia thực hiện cho phép các bên liên quan đẩy nhanh và tối ưu hóa quy trình đánh giá sản phẩm mà họ đánh giá.  Mẫu RFP nhằm mục đích nắm bắt được mẫu số chung nhất về nhu cầu bảo mật và cung cấp các yếu tố cần thiết phù hợp với bất kỳ tổ chức nào.  Một giải pháp XDR có thể mang lại lợi ích cho các công ty lớn đang ngập trong các cảnh báo từ nhiều nguồn phát hiện, hợp lý hóa vô số tín hiệu và đơn giản hóa các hành động phản hồi. Các công ty nhỏ hơn được hưởng lợi bằng cách tận dụng một nền tảng duy nhất mà nếu không sẽ yêu cầu phối hợp một số giải pháp điểm phức tạp và đắt tiền. Về mặt logic, các tổ chức có thể đạt được khả năng hiển thị mối đe dọa lớn hơn cùng với mức độ phức tạp giảm.  Eyal Gruner, Giám đốc điều hành của Cynet cho biết: “Bất chấp tất cả các công cụ bảo mật đã được triển khai trong nhiều năm để ngăn chặn và phát hiện các vi phạm, những kẻ tấn công vẫn có thể tìm thấy các đường nối trong các biện pháp bảo vệ. "Một trong những vấn đề chính là các đội bảo mật đơn giản là không thể hiểu được hàng loạt thông tin và cảnh báo đến với họ từ nhiều công cụ bảo mật. Và, một số tổ chức không đủ khả năng triển khai tất cả các công cụ giám sát cần thiết để đảm bảo bảo vệ đầy đủ. "  Để cung cấp khả năng bảo vệ vi phạm mạnh mẽ, các tổ chức phải thu thập, tổng hợp và hiểu các tín hiệu từ các vectơ tấn công chính như là bước đầu tiên để phòng thủ tốt hơn. Sau đó, tự động hóa điều tra và khắc phục để bao gồm toàn bộ phạm vi của mỗi cuộc tấn công đảm bảo tất cả các hành động thích hợp được thực hiện để bảo vệ tổ chức. Đây là lúc XDR xuất hiện.  Sử dụng các mẫu làm sẵn có thể tiết kiệm đáng kể thời gian và nguồn lực để xây dựng danh sách yêu cầu tương tự từ đầu. Giải pháp RFP của XDR có thể giúp các công ty ưu tiên các khả năng có sẵn trong các giải pháp mới nổi để cải thiện quyết định mua hàng của họ.  RFP bao gồm năm phần:   Giám sát & Kiểm soát — các hoạt động thường xuyên để có được khả năng hiển thị và chủ động phát hiện cũng như giảm các bề mặt tấn công. Phòng ngừa & Phát hiện — cơ chế để ngăn chặn nhiều loại hàng hóa và các vectơ tấn công tiên tiến. Điều tra & phản ứng — một bộ công cụ tổng thể để phản ứng hiệu quả với các cuộc tấn công trực tiếp được phát hiện. Cơ sở hạ tầng — kiến ​​trúc, triển khai, thu thập dữ liệu và giao tiếp. Vận hành — quản lý liên tục giải pháp   Hướng dẫn RFP đảm bảo các tổ chức không bỏ qua các khía cạnh quan trọng của khả năng giải pháp bảo mật và do đó đưa ra các quyết định không chuẩn cho các giao dịch mua quan trọng của doanh nghiệp.  Tải xuống XDR RFP tại đây.   Tìm thấy bài viết này thú vị? Theo dõi THN trên Facebook, Twitter  và LinkedIn để đọc thêm nội dung độc quyền mà chúng tôi đăng. |

# Over 200,000 MicroTik Routers Worldwide Are Under the Control of Botnet Malware

📅Date: March 23, 2022 👤Author: Ravie Lakshmanan

Link tham khảo: *https://thehackernews.com/2022/03/over-200000-microtik-routers-worldwide.html*



|  |  |
| --- | --- |
| Title: 🐄Over 200,000 MicroTik Routers Worldwide Are Under the Control of Botnet Malware | Title: 🐄Hơn 200.000 bộ định tuyến MicroTik trên toàn thế giới đang chịu sự kiểm soát của phần mềm độc hại Botnet |
| Vulnerable routers from MikroTik have been misused to form what cybersecurity researchers have called one of the largest botnet-as-a-service cybercrime operations seen in recent years.  According to a new piece of research published by Avast, a cryptocurrency mining campaign leveraging the new-disrupted Glupteba botnet as well as the infamous TrickBot malware were all distributed using the same command-and-control (C2) server. "The C2 server serves as a botnet-as-a-service controlling nearly 230,000 vulnerable MikroTik routers," Avast's senior malware researcher, Martin Hron, said in a write-up, potentially linking it to what's now called the Mēris botnet.  The botnet is known to exploit a known vulnerability in the Winbox component of MikroTik routers (CVE-2018-14847), enabling the attackers to gain unauthenticated, remote administrative access to any affected device. Parts of the Mēris botnet were sinkholed in late September 2021. "The CVE-2018-14847 vulnerability, which was publicized in 2018, and for which MikroTik issued a fix for, allowed the cybercriminals behind this botnet to enslave all of these routers, and to presumably rent them out as a service," Hron said. In attack chain observed by Avast in July 2021, vulnerable MikroTik routers were targeted to retrieve the first-stage payload from a domain named bestony[.]club, which was then used to fetch additional scripts from a second domain "globalmoby[.]xyz." Interesting enough, both the domains were linked to the same IP address: 116.202.93[.]14, leading to the discovery of seven more domains that were actively used in attacks, one of which (tik.anyget[.]ru) was used to serve Glupteba malware samples to targeted hosts. "When requesting the URL https://tik.anyget[.]ru I was redirected to the https://routers.rip/site/login domain (which is again hidden by the Cloudflare proxy)," Hron said. "This is a control panel for the orchestration of enslaved MikroTik routers," with the page displaying a live counter of devices connected into the botnet. But after details of the Mēris botnet entered public domain in early September 2021, the C2 server is said to have abruptly stopped serving scripts before disappearing completely.  The disclosure also coincides with a new report from Microsoft, which revealed how the TrickBot malware has weaponized MikroTik routers as proxies for command-and-control communications with the remote servers, raising the possibility that the operators may have used the same botnet-as-a-service. In light of these attacks, it's recommended that users update their routers with the latest security patches, set up a strong router password, and disable the router's administration interface from the public side. "It also shows, what is quite obvious for some time already, that IoT devices are being heavily targeted not just to run malware on them, which is hard to write and spread massively considering all the different architectures and OS versions, but to simply use their legal and built-in capabilities to set them up as proxies," Hron said. "This is done to either anonymize the attacker's traces or to serve as a DDoS amplification tool."   Found this article interesting? Follow THN on Facebook, Twitter  and LinkedIn to read more exclusive content we post. | Các bộ định tuyến dễ bị tổn thương của MikroTik đã bị lạm dụng để tạo thành cái mà các nhà nghiên cứu an ninh mạng gọi là một trong những hoạt động của tội phạm mạng botnet dưới dạng dịch vụ lớn nhất được thấy trong những năm gần đây. Theo một nghiên cứu mới được công bố bởi Avast, một chiến dịch khai thác tiền điện tử tận dụng mạng botnet Glupteba mới bị gián đoạn cũng như phần mềm độc hại khét tiếng TrickBot đều được phân phối bằng cùng một máy chủ điều khiển (C2). Nhà nghiên cứu phần mềm độc hại cấp cao của Avast, Martin Hron, cho biết trong một bài viết, có khả năng liên kết nó với mạng botnet Mēris.  Mạng botnet được biết là khai thác một lỗ hổng đã biết trong thành phần Winbox của bộ định tuyến MikroTik (CVE-2018-14847), cho phép những kẻ tấn công có được quyền truy cập quản trị từ xa, chưa được xác thực vào bất kỳ thiết bị bị ảnh hưởng nào. Các phần của mạng botnet Mēris đã bị chìm vào cuối tháng 9 năm 2021. "Lỗ hổng CVE-2018-14847, được công khai vào năm 2018 và MikroTik đã đưa ra bản sửa lỗi cho phép tội phạm mạng đằng sau mạng botnet này làm nô lệ cho tất cả các bộ định tuyến này và có lẽ cho thuê chúng như một dịch vụ", Hron nói . Trong chuỗi tấn công được Avast quan sát vào tháng 7 năm 2021, các bộ định tuyến MikroTik dễ bị tấn công đã được nhắm mục tiêu để truy xuất tải trọng giai đoạn đầu từ miền có tên bestony [.] Club, sau đó được sử dụng để tìm nạp các tập lệnh bổ sung từ miền thứ hai "globalmoby [.] Xyz . " Khá thú vị, cả hai miền đều được liên kết với cùng một địa chỉ IP: 116.202.93 [.] 14, dẫn đến việc phát hiện thêm bảy miền khác được sử dụng tích cực trong các cuộc tấn công, một trong số đó (tik.anyget [.] Ru) là được sử dụng để cung cấp các mẫu phần mềm độc hại Glupteba cho các máy chủ được nhắm mục tiêu. "Khi yêu cầu URL https: //tik.anyget [.] Ru, tôi đã được chuyển hướng đến miền https://routers.rip/site/login (miền này lại bị ẩn bởi proxy Cloudflare)", Hron nói. "Đây là một bảng điều khiển cho việc điều phối các bộ định tuyến MikroTik nô lệ", với trang này hiển thị một bộ đếm trực tiếp của các thiết bị được kết nối với mạng botnet. Nhưng sau khi thông tin chi tiết về mạng botnet Mēris được đưa vào phạm vi công cộng vào đầu tháng 9 năm 2021, máy chủ C2 được cho là đã đột ngột ngừng cung cấp các tập lệnh trước khi biến mất hoàn toàn.  Tiết lộ cũng trùng với một báo cáo mới của Microsoft, trong đó tiết lộ cách phần mềm độc hại TrickBot đã vũ khí hóa các bộ định tuyến MikroTik làm proxy để giao tiếp lệnh và điều khiển với các máy chủ từ xa, làm tăng khả năng các nhà khai thác có thể đã sử dụng cùng một mạng botnet-as- a-dịch vụ. Trước những cuộc tấn công này, người dùng nên cập nhật bộ định tuyến của họ bằng các bản vá bảo mật mới nhất, thiết lập mật khẩu bộ định tuyến mạnh và vô hiệu hóa giao diện quản trị bộ định tuyến từ phía công khai. "Nó cũng cho thấy, điều đã khá rõ ràng trong một thời gian, rằng các thiết bị IoT đang bị nhắm mục tiêu mạnh mẽ không chỉ để chạy phần mềm độc hại trên chúng, khó viết và lây lan hàng loạt xét trên tất cả các kiến ​​trúc và phiên bản hệ điều hành khác nhau, mà chỉ để sử dụng Hron nói. "Điều này được thực hiện để ẩn danh các dấu vết của kẻ tấn công hoặc để phục vụ như một công cụ khuếch đại DDoS."   Tìm thấy bài viết này thú vị? Theo dõi THN trên Facebook, Twitter  và LinkedIn để đọc thêm nội dung độc quyền mà chúng tôi đăng. |

# Microsoft and Okta Confirm Breach by LAPSUS$ Extortion Group

📅Date: March 22, 2022 👤Author: Ravie Lakshmanan

Link tham khảo: *https://thehackernews.com/2022/03/microsoft-and-okta-confirm-breach-by.html*



|  |  |
| --- | --- |
| Title: 🐄Microsoft and Okta Confirm Breach by LAPSUS$ Extortion Group | Title: 🐄Microsoft và Okta Xác nhận Vi phạm bởi Nhóm tống tiền LAPSUS $ |
| Microsoft on Tuesday confirmed that the LAPSUS$ extortion-focused hacking crew had gained "limited access" to its systems, as authentication services provider Okta revealed that nearly 2.5% of its customers have been potentially impacted in the wake of the breach. "No customer code or data was involved in the observed activities," Microsoft's Threat Intelligence Center (MSTIC) said, adding that the breach was facilitated by means of a single compromised account that has since been remediated to prevent further malicious activity. The Windows maker, which was already tracking the group under the moniker DEV-0537 prior to the public disclosure, said it "does not rely on the secrecy of code as a security measure and viewing source code does not lead to elevation of risk." "This public disclosure escalated our action allowing our team to intervene and interrupt the actor mid-operation, limiting broader impact," the company's security teams noted. Identity and access management company Okta, which also acknowledged the breach through the account of a customer support engineer working for a third-party provider, said that the attackers had access to the engineer's laptop during a five-day window between January 16 and 21, but that the service itself was not compromised.  The San Francisco-based cloud software firm also said it's identified the affected customers and that it's contacting them directly, stressing that the "Okta service is fully operational, and there are no corrective actions our customers need to take." "In the case of the Okta compromise, it would not suffice to just change a user's password," web infrastructure company Cloudflare said in a post mortem analysis of the incident. "The attacker would also need to change the hardware (FIDO) token configured for the same user. As a result, it would be easy to spot compromised accounts based on the associated hardware keys." That said, of particular concern is the fact that Okta failed to publicly disclose the breach for two months, prompting the cyber criminal group to ask "Why wait this long?" in its counter statement. LAPSUS$ has also claimed in its rebuttal that Okta was storing Amazon Web Services (AWS) keys within Slack and that support engineers seem to have "excessive access" to the communications platform. "The potential impact to Okta customers is NOT limited, I'm pretty certain resetting passwords and MFA would result in complete compromise of many clients' systems," the gang elaborated. Microsoft Exposes the Tactics of LAPSUS$ LAPSUS$, which first emerged in July 2021, has been on a hacking spree in recent months, targeting a wealth of companies over the intervening period, including Impresa, Brazil's Ministry of Health, Claro, Embratel, NVIDIA, Samsung, Mercado Libre, Vodafone, and most recently Ubisoft. The financially motivated group's modus operandi has been relatively straightforward: break into a target's network, steal sensitive data, and blackmail the victim company into paying up by publicizing snippets of the stolen data on their Telegram channel.  Microsoft described LAPSUS$ as a group following a "pure extortion and destruction model without deploying ransomware payloads" and one that "doesn't seem to cover its tracks." Other tactics adopted by the crew include phone-based social engineering schemes such as SIM-swapping to facilitate account takeover, accessing personal email accounts of employees at target organizations, bribing employees, suppliers, or business partners of companies for access, and intruding in the ongoing crisis-response calls of their targets to initiate extortion demands. LAPSUS$ has also been observed deploying the RedLine Stealer that's available for sale on underground forums to obtain passwords and session tokens, in addition to buying credentials and access tokens from dark web marketplaces as well as searching public code repositories for exposed credentials, to gain an initial foothold.  "The objective of DEV-0537 actors is to gain elevated access through stolen credentials that enable data theft and destructive attacks against a targeted organization, often resulting in extortion," the company said. "Tactics and objectives indicate this is a cybercriminal actor motivated by theft and destruction." Following initial access, the group is known to exploit unpatched vulnerabilities on internally accessible Confluence, JIRA, and GitLab servers for privilege escalation, before proceeding to exfiltrate relevant information and delete the target's systems and resources. To mitigate such incidents, Microsoft is recommending organizations to mandate multi-factor authentication (but not SMS-based), make use of modern authentication options such as OAuth or SAML, review individual sign-ins for signs of anomalous activity, and monitor incident response communications for unauthorized attendees. "Based on observed activity, this group understands the interconnected nature of identities and trust relationships in modern technology ecosystems and targets telecommunications, technology, IT services and support companies – to leverage their access from one organization to access the partner or supplier organizations." Amidst the fallout from the leaks, LAPSUS$ appear to be taking a break. "A few of our members has [sic] a vacation until 30/3/2022. We might be quiet for some times [sic]," the group said on its Telegram channel.   Found this article interesting? Follow THN on Facebook, Twitter  and LinkedIn to read more exclusive content we post. | Microsoft hôm thứ Ba xác nhận rằng nhóm tấn công tập trung vào mã độc tống tiền LAPSUS $ đã có được "quyền truy cập hạn chế" vào hệ thống của họ, vì nhà cung cấp dịch vụ xác thực Okta tiết lộ rằng gần 2,5% khách hàng của họ có khả năng bị ảnh hưởng sau vụ vi phạm. "Không có mã khách hàng hoặc dữ liệu nào liên quan đến các hoạt động được quan sát", Trung tâm Tình báo Đe dọa của Microsoft (MSTIC) cho biết, đồng thời cho biết thêm rằng vi phạm được thực hiện nhờ một tài khoản bị xâm phạm duy nhất đã được khắc phục để ngăn chặn các hoạt động độc hại tiếp theo. Nhà sản xuất Windows, đã theo dõi nhóm với biệt danh DEV-0537 trước khi công bố rộng rãi, cho biết họ "không dựa vào tính bí mật của mã như một biện pháp bảo mật và việc xem mã nguồn không dẫn đến rủi ro cao." "Việc tiết lộ công khai này khiến hành động của chúng tôi leo thang, cho phép nhóm của chúng tôi can thiệp và làm gián đoạn quá trình hoạt động giữa chừng của diễn viên, hạn chế tác động trên diện rộng", nhóm bảo mật của công ty lưu ý. Công ty quản lý danh tính và quyền truy cập Okta, cũng thừa nhận vi phạm thông qua tài khoản của một kỹ sư hỗ trợ khách hàng làm việc cho nhà cung cấp bên thứ ba, nói rằng những kẻ tấn công đã truy cập vào máy tính xách tay của kỹ sư trong khoảng thời gian 5 ngày từ 16 đến 21 tháng 1, nhưng bản thân dịch vụ không bị xâm phạm.  Công ty phần mềm đám mây có trụ sở tại San Francisco cũng cho biết họ đã xác định được những khách hàng bị ảnh hưởng và họ đang liên hệ trực tiếp với họ, nhấn mạnh rằng "dịch vụ Okta đã hoạt động hoàn toàn và không có hành động sửa chữa nào mà khách hàng của chúng tôi cần thực hiện." "Trong trường hợp thỏa hiệp Okta, chỉ cần thay đổi mật khẩu của người dùng là không đủ", công ty cơ sở hạ tầng web Cloudflare cho biết trong một phân tích khám nghiệm tử thi về vụ việc. "Kẻ tấn công cũng sẽ cần thay đổi mã thông báo phần cứng (FIDO) được định cấu hình cho cùng một người dùng. Do đó, sẽ dễ dàng phát hiện các tài khoản bị xâm nhập dựa trên các khóa phần cứng liên quan." Điều đó nói rằng, mối quan tâm đặc biệt là thực tế là Okta đã không công khai hành vi vi phạm trong hai tháng, khiến nhóm tội phạm mạng đặt câu hỏi "Tại sao phải đợi lâu như vậy?" trong tuyên bố phản đối của nó. LAPSUS $ cũng đã tuyên bố trong bài bác bỏ rằng Okta đang lưu trữ các khóa Amazon Web Services (AWS) trong Slack và các kỹ sư hỗ trợ dường như có "quyền truy cập quá mức" vào nền tảng truyền thông. "Tác động tiềm năng đối với khách hàng của Okta là KHÔNG giới hạn, tôi khá chắc chắn rằng việc đặt lại mật khẩu và MFA sẽ dẫn đến sự xâm phạm hoàn toàn hệ thống của nhiều khách hàng", băng nhóm này giải thích. Microsoft tiết lộ các chiến thuật của LAPSUS $ LAPSUS $, xuất hiện lần đầu tiên vào tháng 7 năm 2021, đã tấn công mạnh mẽ trong những tháng gần đây, nhắm mục tiêu vào vô số công ty trong giai đoạn can thiệp, bao gồm Impresa, Bộ Y tế Brazil, Claro, Embratel, NVIDIA, Samsung, Mercado Libre, Vodafone , và gần đây nhất là Ubisoft. Phương thức hoạt động của nhóm có động cơ tài chính tương đối đơn giản: đột nhập vào mạng của mục tiêu, lấy cắp dữ liệu nhạy cảm và tống tiền công ty nạn nhân bằng cách công khai các đoạn dữ liệu bị đánh cắp trên kênh Telegram của họ.  Microsoft đã mô tả LAPSUS $ là một nhóm theo "mô hình tống tiền và phá hủy thuần túy mà không triển khai tải trọng ransomware" và một nhóm "dường như không che giấu được dấu vết của nó." Các chiến thuật khác được phi hành đoàn áp dụng bao gồm các kế hoạch kỹ thuật xã hội dựa trên điện thoại như hoán đổi SIM để tạo điều kiện tiếp quản tài khoản, truy cập tài khoản email cá nhân của nhân viên tại các tổ chức mục tiêu, hối lộ nhân viên, nhà cung cấp hoặc đối tác kinh doanh của công ty để truy cập và xâm nhập vào các cuộc gọi đáp trả khủng hoảng liên tục nhắm vào các mục tiêu của họ để bắt đầu các nhu cầu tống tiền. LAPSUS $ cũng đã được quan sát thấy việc triển khai RedLine Stealer có sẵn để bán trên các diễn đàn ngầm để lấy mật khẩu và mã thông báo phiên, ngoài việc mua thông tin xác thực và mã thông báo truy cập từ các thị trường web tối cũng như tìm kiếm kho mã công khai để tìm thông tin đăng nhập bị lộ, để đạt được chỗ đứng ban đầu.  Công ty cho biết: “Mục tiêu của các tác nhân DEV-0537 là có được quyền truy cập cao hơn thông qua các thông tin đăng nhập bị đánh cắp, cho phép đánh cắp dữ liệu và các cuộc tấn công phá hoại chống lại một tổ chức được nhắm mục tiêu, thường dẫn đến tống tiền,” công ty cho biết. "Các chiến thuật và mục tiêu chỉ ra rằng đây là một kẻ tội phạm mạng được thúc đẩy bởi hành vi trộm cắp và phá hoại." Sau khi truy cập ban đầu, nhóm được biết là khai thác các lỗ hổng chưa được vá trên các máy chủ Confluence, JIRA và GitLab có thể truy cập nội bộ để báo cáo đặc quyền, trước khi tiến hành lọc thông tin liên quan và xóa các hệ thống và tài nguyên của mục tiêu. Để giảm thiểu những sự cố như vậy, Microsoft khuyến nghị các tổ chức bắt buộc xác thực đa yếu tố (nhưng không dựa trên SMS), sử dụng các tùy chọn xác thực hiện đại như OAuth hoặc SAML, xem xét các lần đăng nhập cá nhân để tìm dấu hiệu hoạt động bất thường và theo dõi phản ứng sự cố thông tin liên lạc cho những người tham dự trái phép. "Dựa trên hoạt động được quan sát, nhóm này hiểu được bản chất liên kết của danh tính và mối quan hệ tin cậy trong hệ sinh thái công nghệ hiện đại và nhắm mục tiêu đến các công ty viễn thông, công nghệ, dịch vụ CNTT và hỗ trợ - để tận dụng quyền truy cập của họ từ một tổ chức để tiếp cận các tổ chức đối tác hoặc nhà cung cấp." Giữa bụi phóng xạ do rò rỉ, LAPSUS $ dường như đang tạm nghỉ. "Một số thành viên của chúng tôi [sic] có kỳ nghỉ cho đến ngày 30/3/2022. Chúng tôi có thể sẽ im lặng trong một thời gian [sic]," nhóm cho biết trên kênh Telegram của mình.   Tìm thấy bài viết này thú vị? Theo dõi THN trên Facebook, Twitter  và LinkedIn để đọc thêm nội dung độc quyền mà chúng tôi đăng. |

# LAPSUS$ Hackers Claim to Have Breached Microsoft and Authentication Firm Okta

📅Date: March 22, 2022 👤Author: Ravie Lakshmanan

Link tham khảo: *https://thehackernews.com/2022/03/lapsus-hackers-claim-to-have-breached.html*

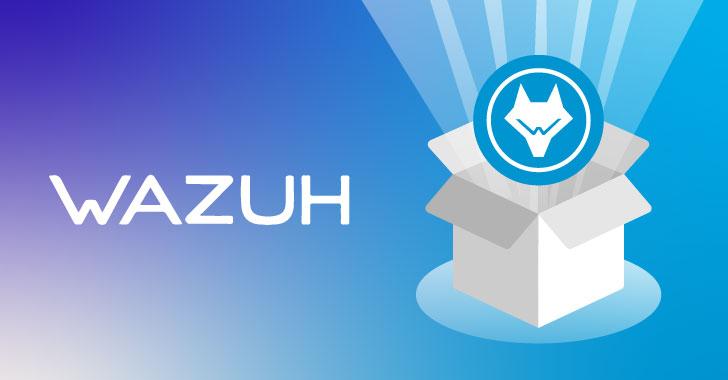


|  |  |
| --- | --- |
| Title: 🐄LAPSUS$ Hackers Claim to Have Breached Microsoft and Authentication Firm Okta | Title: 🐄Tin tặc LAPSUS $ tuyên bố đã xâm phạm Microsoft và công ty xác thực Okta |
| Microsoft and authentication services provider Okta said they are investigating claims of a potential breach alleged by the LAPSUS$ extortionist gang. The development, which was first reported by Vice and Reuters, comes after the cyber criminal group posted screenshots and source code of what it said were the companies' internal projects and systems on its Telegram channel. The leaked 37GB archive shows that the group may have accessed the repositories related to Microsoft's Bing, Bing Maps, and Cortana, with the images highlighting Okta's Atlassian suite and in-house Slack channels.  "For a service that powers authentication systems to many of the largest corporations (and FEDRAMP approved) I think these security measures are pretty poor," the hacking cartel wrote on Telegram. On top of this, the group alleged that it breached LG Electronics (LGE) for the "second time" in a year. Bill Demirkapi, an independent security researcher, noted that "LAPSUS$ appears to have gotten access to the Cloudflare tenant with the ability to reset employee passwords," adding the company "failed to publicly acknowledge any breach for at least two months."  LAPSUS$ has since clarified that it did not breach Okta's databases and that "our focus was ONLY on Okta customers." This could pose serious implications for other government agencies and companies that rely on Okta to authenticate user access to internal systems. "In late January 2022, Okta detected an attempt to compromise the account of a third-party customer support engineer working for one of our subprocessors. The matter was investigated and contained by the subprocessor," Okta CEO Todd McKinnon said in a tweet. "We believe the screenshots shared online are connected to this January event. Based on our investigation to date, there is no evidence of ongoing malicious activity beyond the activity detected in January," McKinnon added. Cloudflare, in response, said it's resetting the Okta credentials of employees who have changed their passwords in the last four months, out of abundance of caution.  Unlike traditional ransomware groups that follow the double extortion playbook of stealing data from a victim and then encrypting that information in return for a payment, the new entrant to the threat landscape focuses more on data theft and using it to blackmail the targets. In the months since it went active in late December 2021, the cybercrime gang has racked up a long list of high-profile victims, including Impresa, NVIDIA, Samsung, Mercado Libre, Vodafone, and most recently Ubisoft. "Any successful attack against a service provider or software developer can have further impact beyond the scope of that initial attack," Mike DeNapoli, lead security architect of Cymulate, said in a statement. "Users of the services and platforms must be alerted to the fact that there are possible supply-chain attacks that will need to be defended against."   Found this article interesting? Follow THN on Facebook, Twitter  and LinkedIn to read more exclusive content we post. | Microsoft và nhà cung cấp dịch vụ xác thực Okta cho biết họ đang điều tra các tuyên bố về một vụ vi phạm tiềm ẩn bị cáo buộc bởi băng đảng tống tiền LAPSUS $. Diễn biến này được Vice và Reuters báo cáo lần đầu tiên diễn ra sau khi nhóm tội phạm mạng đăng ảnh chụp màn hình và mã nguồn của những gì chúng cho là các dự án và hệ thống nội bộ của công ty trên kênh Telegram của chúng. Bản lưu trữ 37GB bị rò rỉ cho thấy nhóm có thể đã truy cập vào các kho lưu trữ liên quan đến Bing, Bing Maps và Cortana của Microsoft, với những hình ảnh làm nổi bật bộ Atlassian của Okta và các kênh Slack nội bộ.  "Đối với một dịch vụ cung cấp hệ thống xác thực cho nhiều tập đoàn lớn nhất (và FEDRAMP đã phê duyệt), tôi nghĩ rằng các biện pháp bảo mật này khá kém", nhóm tấn công viết trên Telegram. Ngoài ra, nhóm còn cáo buộc rằng họ đã vi phạm LG Electronics (LGE) lần thứ hai trong năm. Bill Demirkapi, một nhà nghiên cứu bảo mật độc lập, lưu ý rằng "LAPSUS $ dường như đã có quyền truy cập vào đối tượng thuê Cloudflare với khả năng đặt lại mật khẩu của nhân viên," thêm rằng công ty "đã không công khai thừa nhận bất kỳ vi phạm nào trong ít nhất hai tháng."  LAPSUS $ kể từ đó đã làm rõ rằng nó không vi phạm cơ sở dữ liệu của Okta và rằng "trọng tâm của chúng tôi CHỈ là khách hàng Okta." Điều này có thể gây ra những tác động nghiêm trọng cho các cơ quan chính phủ và các công ty khác dựa vào Okta để xác thực quyền truy cập của người dùng vào các hệ thống nội bộ. "Vào cuối tháng 1 năm 2022, Okta đã phát hiện nỗ lực xâm phạm tài khoản của một kỹ sư hỗ trợ khách hàng bên thứ ba làm việc cho một trong những nhà xử lý phụ của chúng tôi. Vấn đề đã được nhà xử lý phụ điều tra và ngăn chặn", CEO Okta, Todd McKinnon cho biết trong một tweet. "Chúng tôi tin rằng các ảnh chụp màn hình được chia sẻ trực tuyến có liên quan đến sự kiện tháng Giêng này. Dựa trên cuộc điều tra của chúng tôi cho đến nay, không có bằng chứng về hoạt động độc hại đang diễn ra ngoài hoạt động được phát hiện vào tháng Giêng", McKinnon nói thêm. Đáp lại, Cloudflare cho biết họ đang đặt lại thông tin đăng nhập Okta của những nhân viên đã thay đổi mật khẩu của họ trong bốn tháng qua, vì hết sức thận trọng.  Không giống như các nhóm ransomware truyền thống tuân theo vở kịch tống tiền kép là đánh cắp dữ liệu từ nạn nhân và sau đó mã hóa thông tin đó để đổi lấy một khoản thanh toán, kẻ mới tham gia vào bối cảnh mối đe dọa tập trung nhiều hơn vào việc đánh cắp dữ liệu và sử dụng nó để tống tiền các mục tiêu. Trong những tháng kể từ khi hoạt động vào cuối tháng 12 năm 2021, băng nhóm tội phạm mạng đã lập ra một danh sách dài những nạn nhân nổi tiếng, bao gồm Impresa, NVIDIA, Samsung, Mercado Libre, Vodafone và gần đây nhất là Ubisoft. Mike DeNapoli, kiến ​​trúc sư bảo mật hàng đầu của Cymulate, cho biết: “Bất kỳ cuộc tấn công thành công nào chống lại nhà cung cấp dịch vụ hoặc nhà phát triển phần mềm đều có thể gây ra tác động lớn hơn ngoài phạm vi của cuộc tấn công ban đầu đó. "Người dùng các dịch vụ và nền tảng phải được cảnh báo về thực tế rằng có thể có các cuộc tấn công chuỗi cung ứng sẽ cần được bảo vệ chống lại."   Tìm thấy bài viết này thú vị? Theo dõi THN trên Facebook, Twitter  và LinkedIn để đọc thêm nội dung độc quyền mà chúng tôi đăng. |

# Wazuh Offers XDR Functionality at a Price Enterprises Will Love — Free!

📅Date: March 22, 2022 👤Author: The Hacker News

Link tham khảo: *https://thehackernews.com/2022/03/wazuh-offers-xdr-functionality-at-price.html*



|  |  |
| --- | --- |
| Title: 🐄Wazuh Offers XDR Functionality at a Price Enterprises Will Love — Free! | Title: 🐄Wazuh cung cấp chức năng XDR với mức giá mà doanh nghiệp sẽ thích - Miễn phí! |
| Back in 2018, Palo Alto Networks CTO and co-founder Nir Zuk coined a new term to describe the way that businesses needed to approach cybersecurity in the years to come. That term, of course, was extended detection and response (XDR). It described a unified cybersecurity infrastructure that brought endpoint threat detection, network analysis and visibility (NAV), access management, and more under a single roof to find and neutralize digital threats in real-time. And Zuk's vision of XDR proved prophetic. In the years since he coined the phrase, platforms leveraging the XDR model have emerged as the de-facto leaders of the business cybersecurity industry. But their scale and complexity put them in a product class that's just out of reach for some enterprises. Fortunately, the open-source community — as it often does — has filled the XDR void with an affordable product — because it's totally free. It's called Wazuh, and it provides enterprises the tools they need to build a customized XDR solution that meets their cybersecurity and budgetary needs at the same time. Here's how. The Key Features of an XDR Platform Although the varied implementations of XDR solutions come with varying feature sets, most XDR platforms have a few major features in common. They include: Data Analytics and Detection Functionality  Much of the threat detection offered by XDR solutions come in the form of data analytics. By analyzing the logs and performance of major systems, it's often possible to spot abnormal activity or threats. To facilitate this, XDR platforms typically perform analysis of both external and internal traffic, compare performance and log data against known threat profiles, and employ machine learning techniques to detect emerging threat patterns such as those of zero-day attacks. Threat Investigation and Active Response XDR platforms don't only provide businesses with a way to spot potential threats. They also provide tools to help IT specialists investigate those threats and deploy various countermeasures to neutralize them using active responses. To make that possible, most XDR platforms provide a centralized alert system that can group related log alerts from multiple systems into a single UI. That UI can also help administrators respond to alerts by orchestrating responses across a variety of endpoints. Using that functionality, admins can update enterprise-wide security policies in response to a detected attack on a single endpoint. Scalability and Evolutionary Capability Last but not least, XDR platforms make it easy for businesses to integrate new systems, technologies, and endpoints to keep them protected. That means they're built for scalability and interoperability with a wide variety of other vendor-specific technology products. In that way, they're a relatively future-proof solution that grows with a business over time. But they also include machine learning functionalities that help their defensive capabilities adapt to a given technology environment and improve as they work. How Wazuh Delivers XDR Functionality The brilliance of the Wazuh approach to XDR is that it can readily integrate with a variety of other open-source security tools. That means businesses that use it can adapt the system to serve their specific needs without any complex and expensive licensing agreements getting in the way. For example, PDQ Deploy to install software and patches on workstations, AbuseIPDB to detect malicious IP addresses involved in spamming, hacking attempts and DDoS attacks, and URLhaus to detect malicious URLs used for malware distribution. But the core of the Wazuh XDR approach comes in the form of its multi-platform monitoring agent. It's compatible with most devices via its high-level OS support. That means businesses can deploy it to begin collecting endpoint data with very little customization needed. Those agents stream system information back to the Wazuh server, where it performs a variety of anomaly and malware detection routines on it. In that way, administrators gain instant visibility into endpoint security through the server's centralized interface. But that's not all. Through integrations with tools like Suricata and OwlH, administrators get powerful network intrusion detection and visualization functions. That gives them the same kind of situational awareness that other major XDR platforms offer, but without the associated price tag. And the system can even execute automated threat response routines based on network and endpoint data — taking action to stop attacks in their tracks with little to no manual intervention required. And because Wazuh is an open-source solution, it offers the ultimate in scalability and evolutionary capabilities. It can already integrate with security-focused machine learning solutions like Amazon's Macie, giving it stored data surveillance capabilities. But the possibility for additional integrations is endless. That means businesses that opt to use Wazuh as an XDR solution won't be locked into a particular machine learning system, and they can tailor the system's evolutionary capability to their own needs. The Critical Takeaways There's little doubt that today's major XDR solutions represent the current state-of-the-art in business-grade cybersecurity. And their all-encompassing approach to defending digital business infrastructure likely represents the future of it, too. That's because they acknowledge the reality that protecting business data and assets means having true transparency into endpoint operations and allowing for infrastructure-wide responses to threats at a moment's notice. Although XDR will not penetrate the cybersecurity market for a few years due to scaling issues, the fact that an open source solution like Wazuh exists is no small feat. It holds the power to provide meaningful and effective XDR functionality to organizations of all sizes. And it's also flexible enough to adapt to changing business needs and new technology integrations. It's no exaggeration to say it's a true game-changer in the cybersecurity space as it exists today. And best of all — it's free and growing at a rapid pace with the support of the open-source community. All businesses have to do to take advantage of it is to invest in some modest hardware to serve as a control hub, or can simply use Wazuh Cloud. They can use Wazuh to create a bespoke XDR system that's on par with anything now available on the commercial market. And even better, they'll end up with a system that's endlessly customizable and upgradeable — meaning it's a system that businesses can invest in without fear that it will someday be outmoded and obsolete. There aren't many solutions in the world of cybersecurity that can make such a claim — making Wazuh a force to be reckoned with in the XDR market writ large.   Found this article interesting? Follow THN on Facebook, Twitter  and LinkedIn to read more exclusive content we post. | Trở lại năm 2018, CTO của Palo Alto Networks và người đồng sáng lập Nir Zuk đã đặt ra một thuật ngữ mới để mô tả cách thức mà các doanh nghiệp cần để tiếp cận vấn đề an ninh mạng trong những năm tới. Tất nhiên, thuật ngữ đó là phát hiện và phản hồi mở rộng (XDR). Nó mô tả một cơ sở hạ tầng an ninh mạng thống nhất mang lại khả năng phát hiện mối đe dọa điểm cuối, phân tích mạng và khả năng hiển thị (NAV), quản lý truy cập và hơn thế nữa dưới một mái nhà duy nhất để tìm và vô hiệu hóa các mối đe dọa kỹ thuật số trong thời gian thực. Và tầm nhìn của Zuk về XDR đã chứng minh tính tiên tri. Trong những năm kể từ khi ông đặt ra cụm từ này, các nền tảng tận dụng mô hình XDR đã nổi lên như những nhà lãnh đạo thực tế của ngành công nghiệp an ninh mạng kinh doanh. Tuy nhiên, quy mô và độ phức tạp của chúng đã xếp chúng vào loại sản phẩm ngoài tầm với đối với một số doanh nghiệp. May mắn thay, cộng đồng nguồn mở - như thường lệ - đã lấp đầy khoảng trống XDR bằng một sản phẩm giá cả phải chăng - vì nó hoàn toàn miễn phí. Nó được gọi là Wazuh và nó cung cấp cho các doanh nghiệp các công cụ cần thiết để xây dựng một giải pháp XDR tùy chỉnh đáp ứng đồng thời nhu cầu về an ninh mạng và ngân sách của họ. Đây là cách thực hiện. Các tính năng chính của nền tảng XDR Mặc dù các giải pháp XDR được triển khai đa dạng đi kèm với các bộ tính năng khác nhau, hầu hết các nền tảng XDR đều có một vài điểm chung chính. Chúng bao gồm: Phân tích dữ liệu và chức năng phát hiện  Phần lớn khả năng phát hiện mối đe dọa được cung cấp bởi các giải pháp XDR ở dạng phân tích dữ liệu. Bằng cách phân tích nhật ký và hiệu suất của các hệ thống chính, thường có thể phát hiện ra các hoạt động bất thường hoặc các mối đe dọa. Để tạo điều kiện thuận lợi cho việc này, các nền tảng XDR thường thực hiện phân tích cả lưu lượng truy cập bên ngoài và bên trong, so sánh hiệu suất và dữ liệu ghi nhật ký dựa trên các cấu hình mối đe dọa đã biết và sử dụng các kỹ thuật máy học để phát hiện các mẫu đe dọa mới nổi, chẳng hạn như các cuộc tấn công zero-day. Điều tra mối đe dọa và phản ứng tích cực Nền tảng XDR không chỉ cung cấp cho các doanh nghiệp cách phát hiện các mối đe dọa tiềm ẩn. Họ cũng cung cấp các công cụ để giúp các chuyên gia CNTT điều tra các mối đe dọa đó và triển khai các biện pháp đối phó khác nhau để vô hiệu hóa chúng bằng cách sử dụng các phản ứng tích cực. Để làm được điều đó, hầu hết các nền tảng XDR đều cung cấp một hệ thống cảnh báo tập trung có thể nhóm các cảnh báo nhật ký liên quan từ nhiều hệ thống thành một giao diện người dùng duy nhất. Giao diện người dùng đó cũng có thể giúp quản trị viên phản hồi các cảnh báo bằng cách sắp xếp các phản hồi trên nhiều điểm cuối khác nhau. Sử dụng chức năng đó, quản trị viên có thể cập nhật các chính sách bảo mật trong toàn doanh nghiệp để đối phó với một cuộc tấn công được phát hiện vào một điểm cuối duy nhất. Khả năng mở rộng và Khả năng tiến hóa Cuối cùng nhưng không kém phần quan trọng, nền tảng XDR giúp các doanh nghiệp dễ dàng tích hợp các hệ thống, công nghệ và thiết bị đầu cuối mới để giữ cho chúng được bảo vệ. Điều đó có nghĩa là chúng được xây dựng để có khả năng mở rộng và khả năng tương tác với nhiều loại sản phẩm công nghệ dành riêng cho nhà cung cấp khác. Theo cách đó, chúng là một giải pháp tương đối phù hợp với tương lai và phát triển cùng với doanh nghiệp theo thời gian. Nhưng chúng cũng bao gồm các chức năng học máy giúp khả năng phòng thủ của chúng thích ứng với môi trường công nghệ nhất định và cải thiện khi chúng hoạt động. Cách Wazuh cung cấp chức năng XDR Điểm nổi bật của phương pháp Wazuh đối với XDR là nó có thể dễ dàng tích hợp với nhiều công cụ bảo mật mã nguồn mở khác. Điều đó có nghĩa là các doanh nghiệp sử dụng nó có thể điều chỉnh hệ thống để phục vụ các nhu cầu cụ thể của họ mà không có bất kỳ thỏa thuận cấp phép phức tạp và tốn kém nào cản trở. Ví dụ: PDQ Deploy để cài đặt phần mềm và bản vá trên máy trạm, AbuseIPDB để phát hiện các địa chỉ IP độc hại liên quan đến việc gửi thư rác, cố gắng lấy cắp dữ liệu và tấn công DDoS, và URLhaus để phát hiện các URL độc hại được sử dụng để phát tán phần mềm độc hại. Nhưng cốt lõi của phương pháp Wazuh XDR nằm ở dạng tác nhân giám sát đa nền tảng của nó. Nó tương thích với hầu hết các thiết bị thông qua hỗ trợ hệ điều hành cấp cao. Điều đó có nghĩa là các doanh nghiệp có thể triển khai nó để bắt đầu thu thập dữ liệu điểm cuối với rất ít tùy chỉnh cần thiết. Các tác nhân đó truyền thông tin hệ thống trở lại máy chủ Wazuh, nơi nó thực hiện nhiều quy trình phát hiện bất thường và phần mềm độc hại trên đó. Bằng cách đó, quản trị viên có được khả năng hiển thị tức thì về bảo mật điểm cuối thông qua giao diện tập trung của máy chủ. Nhưng đó không phải là tất cả. Thông qua tích hợp với các công cụ như Suricata và OwlH, quản trị viên có được các chức năng phát hiện và hình dung xâm nhập mạng mạnh mẽ. Điều đó mang lại cho họ cùng một loại nhận thức tình huống mà các nền tảng XDR lớn khác cung cấp, nhưng không có thẻ giá liên quan. Và hệ thống thậm chí có thể thực hiện các quy trình phản hồi mối đe dọa tự động dựa trên dữ liệu mạng và điểm cuối - thực hiện hành động để ngăn chặn các cuộc tấn công theo dõi của chúng mà không cần can thiệp thủ công hoặc ít. Và bởi vì Wazuh là một giải pháp mã nguồn mở, nó cung cấp khả năng mở rộng và khả năng tiến hóa tối ưu. Nó đã có thể tích hợp với các giải pháp học máy tập trung vào bảo mật như Macie của Amazon, mang lại cho nó khả năng giám sát dữ liệu được lưu trữ. Nhưng khả năng tích hợp bổ sung là vô tận. Điều đó có nghĩa là các doanh nghiệp chọn sử dụng Wazuh làm giải pháp XDR sẽ không bị khóa vào một hệ thống học máy cụ thể và họ có thể điều chỉnh khả năng tiến hóa của hệ thống theo nhu cầu của riêng mình. Các bài học rút ra quan trọng Có chút nghi ngờ rằng các giải pháp XDR chính ngày nay đại diện cho trạng thái tiên tiến nhất hiện nay trong lĩnh vực an ninh mạng cấp doanh nghiệp. Và cách tiếp cận toàn diện của họ để bảo vệ cơ sở hạ tầng kinh doanh kỹ thuật số có thể cũng đại diện cho tương lai của nó. Đó là bởi vì họ thừa nhận thực tế rằng việc bảo vệ dữ liệu và tài sản của doanh nghiệp có nghĩa là phải có sự minh bạch thực sự đối với các hoạt động của điểm cuối và cho phép phản ứng trên toàn cơ sở hạ tầng đối với các mối đe dọa ngay lập tức. Mặc dù XDR sẽ không thâm nhập vào thị trường an ninh mạng trong một vài năm do các vấn đề về quy mô, nhưng thực tế là một giải pháp mã nguồn mở như Wazuh tồn tại là một kỳ tích không nhỏ. Nó có khả năng cung cấp chức năng XDR có ý nghĩa và hiệu quả cho các tổ chức thuộc mọi quy mô. Và nó cũng đủ linh hoạt để thích ứng với nhu cầu kinh doanh thay đổi và tích hợp công nghệ mới. Không quá lời khi nói rằng đó là một kẻ thay đổi cuộc chơi thực sự trong không gian an ninh mạng như ngày nay. Và trên hết - nó miễn phí và đang phát triển với tốc độ nhanh chóng với sự hỗ trợ của cộng đồng mã nguồn mở. Tất cả những gì doanh nghiệp phải làm để tận dụng lợi thế của nó là đầu tư vào một số phần cứng khiêm tốn để phục vụ như một trung tâm điều khiển, hoặc có thể đơn giản là sử dụng Wazuh Cloud. Họ có thể sử dụng Wazuh để tạo ra một hệ thống XDR đặt trước ngang bằng với bất kỳ thứ gì hiện có trên thị trường thương mại. Và thậm chí tốt hơn, họ sẽ kết thúc với một hệ thống có thể tùy chỉnh và nâng cấp liên tục - có nghĩa là đó là một hệ thống mà các doanh nghiệp có thể đầu tư vào mà không sợ rằng một ngày nào đó nó sẽ lỗi thời và lỗi thời. Không có nhiều giải pháp trong thế giới an ninh mạng có thể đưa ra tuyên bố như vậy - khiến Wazuh trở thành một thế lực đáng nể trong thị trường XDR.   Tìm thấy bài viết này thú vị? Theo dõi THN trên Facebook, Twitter  và LinkedIn để đọc thêm nội dung độc quyền mà chúng tôi đăng. |

# U.S. Government Warns Companies of Potential Russian Cyber Attacks

📅Date: March 22, 2022 👤Author: Ravie Lakshmanan

Link tham khảo: *https://thehackernews.com/2022/03/us-government-warns-companies-of.html*

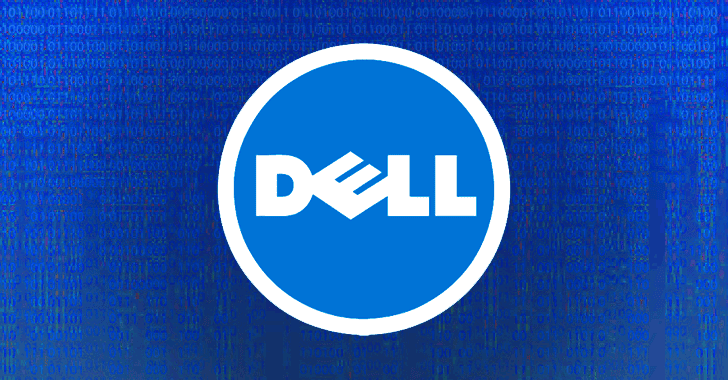


|  |  |
| --- | --- |
| Title: 🐄U.S. Government Warns Companies of Potential Russian Cyber Attacks | Title: 🐄Chính phủ Hoa Kỳ cảnh báo các công ty về các cuộc tấn công mạng tiềm tàng của Nga |
| The U.S. government on Monday once again cautioned of potential cyber attacks from Russia in retaliation for economic sanctions imposed by the west on the country following its military assault on Ukraine last month. "It's part of Russia's playbook," U.S. President Joe Biden said in a statement, citing "evolving intelligence that the Russian Government is exploring options." The development comes as the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) warned of "possible threats" to U.S. and international satellite communication (SATCOM) networks in the wake of a cyber attack targeting Viasat KA-SAT network, used extensively by the Ukrainian military, roughly around the time when Russian armed forces invaded Ukraine on February 24. "Successful intrusions into SATCOM networks could create risk in SATCOM network providers' customer environments," the agencies said.  To strengthen cybersecurity defenses against malicious cyber activity, the government is recommending organizations to mandate the use of multi-factor authentication, ensure that systems are up-to-date and patched against all known vulnerabilities, encrypt data at rest, and maintain offline backups. "Build security into your products from the ground up — 'bake it in, don't bolt it on' — to protect both your intellectual property and your customers' privacy," the U.S. government noted, while also urging companies to scrutinize the provenance of software components, open-source or otherwise, to watch out for supply chain threats. CERT-UA Sounds the Alarm The warnings about spillover incidents follow a barrage of cyber attacks that have struck both Ukraine and Russia over the past few weeks (although they have been quite muted compared to the contrary). Russia, for its part, has urged domestic firms to turn off automatic software updates and switch to Russian DNS servers. Last week, Ukraine's Computer Emergency Response Team (CERT-UA) also notified of new spear-phishing campaigns targeting state entities with the goal of deploying a backdoor called LoadEdge. The agency attributed the attacks to InvisiMole, a hacking crew with suspected ties to the Russia-based nation state group Gamaredon. Separately, the CERT-UA alerted that information systems of Ukrainian enterprises are being compromised by C#-based wiper program called DoubleZero that's engineered to overwrite all non-system files and render the machines inoperable. Spam campaigns piggybacking on the war in Ukraine have also materialized in other ways, some of which leverage charity-themed lures in an attempt to steal money and compromise victims' devices from across the world, once again indicating that cybercrooks are adept at tailoring their schemes for maximum impact. "86% of the fraudulent messages were sent from IP addresses in Lithuania, ending up in inboxes in South Korea (40%), Czech Republic (16%), Germany (7%), the US and UK (5% each), India (4%), Romania, and Italy (2% each)," cybersecurity firm Bitdefender said. What's more, the emerging trend of using "protestware" to poison widely-used open-source libraries as a way of condemning the war has led to fears that it could risk damaging critical systems and undermine confidence in the security of the software supply chain and the open-source ecosystem.  As a consequence, Russian state-owned bank Sberbank has advised users to temporarily abandon software updates, in addition to calling on "developers to increase control over the use of external source code [and] conduct a manual or automated check, including viewing the text of the source code," according to state news service TASS. Conti Version 3 Leaks That's not all. The Russian invasion of Ukraine has also manifested in the form of crowdsourced hacktivist efforts to participate in a variety of digital actions against Russia, primarily leaning on DDoS attacks and publishing troves of sensitive corporate information. Foremost in the list is an anonymous Ukrainian security researcher dubbed @ContiLeaks, who leaked the source code of the Russia-based Conti ransomware, including the more recent "version 3," as well as nearly 170,000 internal chat conversations between the gang members earlier this month, after the group sided with Russia.  In related news, Moscow's Tverskoy district court outlawed Meta-owned social media platforms Facebook and Instagram for engaging in "extremist activities," banning the company from doing business in the country with immediate effect. The ruling follows a temporary decision on part of Meta allowing users in Eastern Europe to post content calling for violence against Russian soldiers.   Found this article interesting? Follow THN on Facebook, Twitter  and LinkedIn to read more exclusive content we post. | Chính phủ Mỹ hôm thứ Hai một lần nữa cảnh báo về các cuộc tấn công mạng tiềm tàng từ Nga để trả đũa các lệnh trừng phạt kinh tế mà phương Tây áp đặt lên nước này sau cuộc tấn công quân sự vào Ukraine hồi tháng trước. "Đó là một phần trong vở kịch của Nga", Tổng thống Mỹ Joe Biden cho biết trong một tuyên bố, với lý do "những thông tin tình báo đang phát triển cho thấy Chính phủ Nga đang khám phá các lựa chọn." Diễn biến này diễn ra khi Cơ quan An ninh mạng và Cơ sở hạ tầng (CISA) và Cục Điều tra Liên bang (FBI) cảnh báo về "các mối đe dọa có thể xảy ra" đối với mạng liên lạc vệ tinh (SATCOM) của Hoa Kỳ và quốc tế sau một cuộc tấn công mạng nhắm vào Viasat KA-SAT. , được sử dụng rộng rãi bởi quân đội Ukraine, vào khoảng thời gian các lực lượng vũ trang Nga xâm lược Ukraine vào ngày 24 tháng Hai. Các cơ quan cho biết: “Việc xâm nhập thành công vào mạng SATCOM có thể tạo ra rủi ro trong môi trường khách hàng của các nhà cung cấp mạng SATCOM.  Để tăng cường khả năng phòng thủ an ninh mạng chống lại hoạt động mạng độc hại, chính phủ khuyến nghị các tổ chức bắt buộc sử dụng xác thực đa yếu tố, đảm bảo rằng các hệ thống được cập nhật và vá chống lại tất cả các lỗ hổng đã biết, mã hóa dữ liệu ở trạng thái nghỉ và duy trì các bản sao lưu ngoại tuyến. Chính phủ Hoa Kỳ lưu ý: "Hãy xây dựng tính bảo mật cho các sản phẩm của bạn ngay từ đầu - 'nướng nó vào, đừng cài nó vào' - để bảo vệ cả tài sản trí tuệ và quyền riêng tư của khách hàng của bạn", chính phủ Hoa Kỳ lưu ý, đồng thời kêu gọi các công ty xem xét kỹ lưỡng nguồn gốc xuất xứ của các thành phần phần mềm, mã nguồn mở hoặc cách khác, để đề phòng các mối đe dọa từ chuỗi cung ứng. CERT-UA phát âm báo Các cảnh báo về các sự cố lan rộng theo sau một loạt các cuộc tấn công mạng đã xảy ra ở cả Ukraine và Nga trong vài tuần qua (mặc dù chúng khá im lặng so với ngược lại). Về phần mình, Nga đã kêu gọi các công ty trong nước tắt cập nhật phần mềm tự động và chuyển sang máy chủ DNS của Nga. Tuần trước, Nhóm Ứng cứu Khẩn cấp Máy tính của Ukraine (CERT-UA) cũng đã thông báo về các chiến dịch lừa đảo mới nhằm vào các tổ chức nhà nước với mục tiêu triển khai một cửa hậu có tên là LoadEdge. Cơ quan này cho rằng các cuộc tấn công là do InvisiMole, một nhóm tấn công bị nghi ngờ có quan hệ với tập đoàn quốc gia Gamaredon có trụ sở tại Nga. Riêng biệt, CERT-UA cảnh báo rằng hệ thống thông tin của các doanh nghiệp Ukraine đang bị xâm nhập bởi chương trình gạt nước dựa trên C # có tên là DoubleZero được thiết kế để ghi đè tất cả các tệp không thuộc hệ thống và khiến máy móc không thể hoạt động. Các chiến dịch thư rác cõng về cuộc chiến ở Ukraine cũng đã hiện thực hóa theo những cách khác, một số trong số đó tận dụng các chiêu dụ từ thiện có chủ đề nhằm đánh cắp tiền và xâm phạm thiết bị của nạn nhân trên khắp thế giới, một lần nữa cho thấy rằng cybercrook rất giỏi trong việc điều chỉnh các âm mưu của chúng để có tác động tối đa. "86% tin nhắn lừa đảo được gửi từ các địa chỉ IP ở Lithuania, cuối cùng được gửi đến các hộp thư đến ở Hàn Quốc (40%), Cộng hòa Séc (16%), Đức (7%), Mỹ và Anh (5% mỗi hộp thư đến), Ấn Độ (4%), Romania và Ý (2% mỗi nước), "công ty an ninh mạng Bitdefender cho biết. Hơn nữa, xu hướng đang nổi lên của việc sử dụng "phần mềm phản đối" để đầu độc các thư viện mã nguồn mở được sử dụng rộng rãi như một cách để lên án chiến tranh đã dẫn đến lo ngại rằng nó có thể có nguy cơ làm hỏng các hệ thống quan trọng và làm suy yếu niềm tin vào tính bảo mật của chuỗi cung ứng phần mềm và hệ sinh thái mã nguồn mở.  Do đó, ngân hàng nhà nước Sberbank của Nga đã khuyến cáo người dùng tạm thời từ bỏ các bản cập nhật phần mềm, bên cạnh việc kêu gọi "các nhà phát triển tăng cường kiểm soát việc sử dụng mã nguồn bên ngoài [và] tiến hành kiểm tra thủ công hoặc tự động, bao gồm cả việc xem văn bản của mã nguồn, "theo dịch vụ tin tức nhà nước TASS. Phiên bản Conti 3 Rò rỉ Đó không phải là tất cả. Cuộc xâm lược của Nga vào Ukraine cũng thể hiện dưới hình thức những nỗ lực của những kẻ tấn công có nguồn lực từ cộng đồng để tham gia vào nhiều hành động kỹ thuật số chống lại Nga, chủ yếu dựa vào các cuộc tấn công DDoS và xuất bản hàng loạt thông tin nhạy cảm của công ty. Đứng đầu danh sách là một nhà nghiên cứu bảo mật ẩn danh người Ukraine có tên là @ContiLeaks, người đã làm rò rỉ mã nguồn của ransomware Conti có trụ sở tại Nga, bao gồm "phiên bản 3" gần đây hơn cũng như gần 170.000 cuộc trò chuyện nội bộ giữa các thành viên băng đảng trước đó. tháng, sau khi nhóm đứng về phía Nga. Trong tin tức liên quan, tòa án quận Tverskoy của Moscow đã cấm các nền tảng mạng xã hội Facebook và Instagram thuộc sở hữu của Meta vì tham gia vào "các hoạt động cực đoan", cấm công ty kinh doanh tại quốc gia này có hiệu lực ngay lập tức. Phán quyết này theo sau một quyết định tạm thời của Meta cho phép người dùng ở Đông Âu đăng nội dung kêu gọi bạo lực đối với binh lính Nga.   Tìm thấy bài viết này thú vị? Theo dõi THN trên Facebook, Twitter  và LinkedIn để đọc thêm nội dung độc quyền mà chúng tôi đăng. |

# New Dell BIOS Bugs Affect Millions of Inspiron, Vostro, XPS, Alienware Systems

📅Date: March 22, 2022 👤Author: Ravie Lakshmanan

Link tham khảo: *https://thehackernews.com/2022/03/new-dell-bios-bugs-affect-millions-of.html*

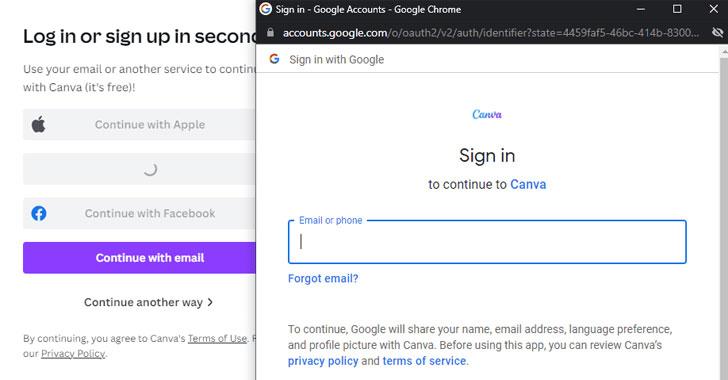


|  |  |
| --- | --- |
| Title: 🐄New Dell BIOS Bugs Affect Millions of Inspiron, Vostro, XPS, Alienware Systems | Title: 🐄Lỗi BIOS mới của Dell ảnh hưởng đến hàng triệu hệ thống Inspiron, Vostro, XPS, Alienware |
| Five new security weaknesses have been disclosed in Dell BIOS that, if successfully exploited, could lead to code execution on vulnerable systems, joining the likes of firmware vulnerabilities recently uncovered in Insyde Software's InsydeH2O and HP Unified Extensible Firmware Interface (UEFI). Tracked as CVE-2022-24415, CVE-2022-24416, CVE-2022-24419, CVE-2022-24420, and CVE-2022-24421, the high-severity vulnerabilities are rated 8.2 out of 10 on the CVSS scoring system. "The active exploitation of all the discovered vulnerabilities can't be detected by firmware integrity monitoring systems due to limitations of the Trusted Platform Module (TPM) measurement," firmware security company Binarly, which discovered the latter three flaws, said in a write-up.  "The remote device health attestation solutions will not detect the affected systems due to the design limitations in visibility of the firmware runtime." All the flaws relate to improper input validation vulnerabilities affecting the System Management Mode (SMM) of the firmware, effectively allowing a local authenticated attacker to leverage the system management interrupt (SMI) to achieve arbitrary code execution. System Management Mode refers to a special-purpose CPU mode in x86 microcontrollers that's designed for handling system-wide functions like power management, system hardware control, thermal monitoring, and other proprietary manufacturer-developed code. Whenever one of these operations is requested, a non-maskable interrupt (SMI) is invoked at runtime, which executes SMM code installed by the BIOS. Given that SMM code executes at the highest privilege level and is invisible to the underlying operating system, the method makes it ripe for abuse to deploy persistent firmware implants.  A number of Dell products, including Alienware, Inspiron, Vostro line-ups, and Edge Gateway 3000 Series, are impacted, with the Texas-headquartered PC manufacturer recommending customers to upgrade their BIOS at the "earliest opportunity." "The ongoing discovery of these vulnerabilities demonstrate what we describe as 'repeatable failures' around the lack of input sanitation or, in general, insecure coding practices," Binarly researchers said. "These failures are a direct consequence of the complexity of the codebase or support for legacy components that get less security attention, but are still widely deployed in the field. In many cases, the same vulnerability can be fixed over multiple iterations, and still, the complexity of the attack surface leaves open gaps for malicious exploitation."   Found this article interesting? Follow THN on Facebook, Twitter  and LinkedIn to read more exclusive content we post. | Năm điểm yếu bảo mật mới đã được tiết lộ trong Dell BIOS, nếu khai thác thành công, có thể dẫn đến việc thực thi mã trên các hệ thống dễ bị tấn công, tham gia vào các lỗ hổng phần mềm tương tự được phát hiện gần đây trong Insyde Software's InsydeH2O và HP Unified Extensible Firmware Interface (UEFI). Được theo dõi là CVE-2022-24415, CVE-2022-24416, CVE-2022-24419, CVE-2022-24420 và CVE-2022-24421, các lỗ hổng có mức độ nghiêm trọng cao được xếp hạng 8,2 trên 10 trên hệ thống tính điểm CVSS. "Việc khai thác tích cực tất cả các lỗ hổng được phát hiện không thể được phát hiện bởi các hệ thống giám sát tính toàn vẹn phần sụn do các hạn chế của phép đo Mô-đun nền tảng đáng tin cậy (TPM)", công ty bảo mật phần sụn Binarly, công ty đã phát hiện ra ba lỗ hổng sau, cho biết trong một bài viết- hướng lên.  "Các giải pháp chứng thực tình trạng thiết bị từ xa sẽ không phát hiện các hệ thống bị ảnh hưởng do các giới hạn thiết kế trong khả năng hiển thị của thời gian chạy chương trình cơ sở." Tất cả các lỗ hổng liên quan đến lỗ hổng xác thực đầu vào không đúng ảnh hưởng đến Chế độ quản lý hệ thống (SMM) của phần sụn, cho phép kẻ tấn công xác thực cục bộ tận dụng ngắt quản lý hệ thống (SMI) để thực thi mã tùy ý. Chế độ quản lý hệ thống đề cập đến chế độ CPU có mục đích đặc biệt trong vi điều khiển x86 được thiết kế để xử lý các chức năng toàn hệ thống như quản lý nguồn, điều khiển phần cứng hệ thống, giám sát nhiệt và các mã độc quyền khác do nhà sản xuất phát triển. Bất cứ khi nào một trong những hoạt động này được yêu cầu, một ngắt không thể che giấu (SMI) được gọi trong thời gian chạy, thực thi mã SMM được cài đặt bởi BIOS. Cho rằng mã SMM thực thi ở mức đặc quyền cao nhất và không thể nhìn thấy đối với hệ điều hành cơ bản, phương pháp này khiến cho việc lạm dụng triển khai cấy ghép phần sụn liên tục đã trở nên chín muồi.  Một số sản phẩm của Dell, bao gồm Alienware, Inspiron, dòng sản phẩm Vostro và Edge Gateway 3000 Series, bị ảnh hưởng, trong đó nhà sản xuất PC có trụ sở tại Texas khuyến nghị khách hàng nên nâng cấp BIOS của họ trong "cơ hội sớm nhất". Các nhà nghiên cứu của Binarly cho biết: “Việc liên tục phát hiện ra những lỗ hổng này chứng minh những gì chúng tôi mô tả là 'những lỗi có thể lặp lại' xung quanh việc thiếu vệ sinh đầu vào hoặc nói chung là các hoạt động mã hóa không an toàn". "Những lỗi này là hậu quả trực tiếp của sự phức tạp của cơ sở mã hoặc hỗ trợ cho các thành phần kế thừa ít được chú ý về bảo mật hơn, nhưng vẫn được triển khai rộng rãi trong lĩnh vực này. Trong nhiều trường hợp, cùng một lỗ hổng có thể được sửa qua nhiều lần lặp lại và vẫn còn, sự phức tạp của bề mặt tấn công để lại những khoảng trống cho việc khai thác ác ý. "   Tìm thấy bài viết này thú vị? Theo dõi THN trên Facebook, Twitter  và LinkedIn để đọc thêm nội dung độc quyền mà chúng tôi đăng. |

# New Browser-in-the Browser (BITB) Attack Makes Phishing Nearly Undetectable

📅Date: March 21, 2022 👤Author: Ravie Lakshmanan

Link tham khảo: *https://thehackernews.com/2022/03/new-browser-in-browser-bitb-attack.html*

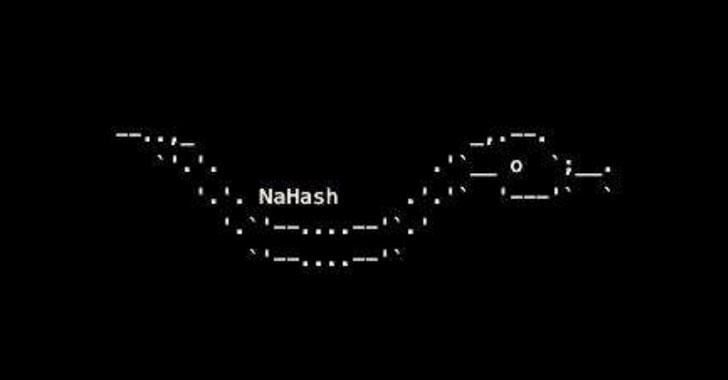


|  |  |
| --- | --- |
| Title: 🐄New Browser-in-the Browser (BITB) Attack Makes Phishing Nearly Undetectable | Title: 🐄Tấn công trình duyệt mới trong trình duyệt (BITB) khiến cho hành vi lừa đảo gần như không thể phát hiện được |
| A novel phishing technique called browser-in-the-browser (BitB) attack can be exploited to simulate a browser window within the browser in order to spoof a legitimate domain, thereby making it possible to stage convincing phishing attacks. According to penetration tester and security researcher, who goes by the handle mrd0x on Twitter, the method takes advantage of third-party single sign-on (SSO) options embedded on websites such as "Sign in with Google" (or Facebook, Apple, or Microsoft).  While the default behavior when a user attempts to sign in via these methods is to be greeted by a pop-up window to complete the authentication process, the BitB attack aims to replicate this entire process using a mix of HTML and CSS code to create an entirely fabricated browser window.  "Combine the window design with an iframe pointing to the malicious server hosting the phishing page, and it's basically indistinguishable," mrd0x said in a technical write-up published last week. "JavaScript can be easily used to make the window appear on a link or button click, on the page loading etc." Interestingly, the technique has been abused in the wild at least once before. In February 2020, Zscaler disclosed details of a campaign that leveraged the BitB trick to siphon credentials for video game digital distribution service Steam by means of fake Counter-Strike: Global Offensive (CS: GO) websites.  "Normally, the measures taken by a user to detect a phishing site include checking to see if the URL is legitimate, whether the website is using HTTPS, and whether there is any kind of homograph in the domain, among others," Zscaler researcher Prakhar Shrotriya said at the time. "In this case, everything looks fine as the domain is steamcommunity[.]com, which is legitimate and is using HTTPS. But when we try to drag this prompt from the currently used window, it disappears beyond the edge of the window as it is not a legitimate browser pop-up and is created using HTML in the current window." While this method significantly makes it easier to mount effective social engineering campaigns, it's worth noting that potential victims need to be redirected to a phishing domain that can display such a fake authentication window for credential harvesting. "But once landed on the attacker-owned website, the user will be at ease as they type their credentials away on what appears to be the legitimate website (because the trustworthy URL says so)," mrd0x added.   Found this article interesting? Follow THN on Facebook, Twitter  and LinkedIn to read more exclusive content we post. | Một kỹ thuật lừa đảo mới được gọi là tấn công trình duyệt trong trình duyệt (BitB) có thể được khai thác để mô phỏng một cửa sổ trình duyệt trong trình duyệt nhằm giả mạo một miền hợp pháp, do đó có thể tạo ra các cuộc tấn công lừa đảo thuyết phục. Theo nhà nghiên cứu bảo mật và kiểm tra thâm nhập, người sử dụng mrd0x trên Twitter, phương pháp này tận dụng các tùy chọn đăng nhập một lần (SSO) của bên thứ ba được nhúng trên các trang web như "Đăng nhập bằng Google" (hoặc Facebook, Apple, hoặc Microsoft).  Mặc dù hành vi mặc định khi người dùng cố gắng đăng nhập thông qua các phương thức này là được chào đón bởi một cửa sổ bật lên để hoàn tất quá trình xác thực, cuộc tấn công BitB nhằm mục đích sao chép toàn bộ quá trình này bằng cách sử dụng kết hợp mã HTML và CSS để tạo ra một cửa sổ trình duyệt hoàn toàn được chế tạo.  "Kết hợp thiết kế cửa sổ với một iframe trỏ đến máy chủ độc hại lưu trữ trang lừa đảo và về cơ bản không thể phân biệt được", mrd0x cho biết trong một bài viết kỹ thuật được xuất bản vào tuần trước. "JavaScript có thể dễ dàng được sử dụng để làm cho cửa sổ xuất hiện trên một liên kết hoặc nhấp vào nút, khi tải trang, v.v." Điều thú vị là kỹ thuật này đã bị lạm dụng trong tự nhiên ít nhất một lần trước đây. Vào tháng 2 năm 2020, Zscaler đã tiết lộ chi tiết về một chiến dịch sử dụng thủ thuật BitB để bòn rút thông tin xác thực cho dịch vụ phân phối trò chơi điện tử kỹ thuật số Steam bằng các trang web giả mạo Counter-Strike: Global Offensive (CS: GO).  "Thông thường, các biện pháp mà người dùng thực hiện để phát hiện một trang web lừa đảo bao gồm kiểm tra xem URL có hợp pháp không, liệu trang web có đang sử dụng HTTPS hay không và liệu có bất kỳ loại đồng nhất nào trong miền hay không," nhà nghiên cứu Prakhar của Zscaler Shrotriya nói vào thời điểm đó. "Trong trường hợp này, mọi thứ có vẻ ổn vì miền là steamcommunity [.] Com, hợp pháp và đang sử dụng HTTPS. Nhưng khi chúng tôi cố gắng kéo lời nhắc này khỏi cửa sổ hiện đang được sử dụng, nó sẽ biến mất ngoài rìa cửa sổ. không phải là cửa sổ bật lên của trình duyệt hợp pháp và được tạo bằng HTML trong cửa sổ hiện tại. " Mặc dù phương pháp này giúp dễ dàng hơn trong việc thực hiện các chiến dịch kỹ thuật xã hội hiệu quả, nhưng cần lưu ý rằng các nạn nhân tiềm năng cần được chuyển hướng đến một miền lừa đảo có thể hiển thị một cửa sổ xác thực giả mạo như vậy để thu thập thông tin đăng nhập. "Nhưng khi đã truy cập vào trang web do kẻ tấn công sở hữu, người dùng sẽ cảm thấy thoải mái khi họ nhập thông tin đăng nhập của họ vào những gì có vẻ là trang web hợp pháp (vì URL đáng tin cậy cho biết như vậy)", mrd0x nói thêm.   Tìm thấy bài viết này thú vị? Theo dõi THN trên Facebook, Twitter  và LinkedIn để đọc thêm nội dung độc quyền mà chúng tôi đăng. |

# New Backdoor Targets French Entities via Open-Source Package Installer

📅Date: March 21, 2022 👤Author: Ravie Lakshmanan

Link tham khảo: *https://thehackernews.com/2022/03/new-backdoor-targets-french-entities.html*



|  |  |
| --- | --- |
| Title: 🐄New Backdoor Targets French Entities via Open-Source Package Installer | Title: 🐄Backdoor mới nhắm mục tiêu các thực thể tiếng Pháp thông qua trình cài đặt gói mã nguồn mở |
| Researchers have exposed a new targeted email campaign aimed at French entities in the construction, real estate, and government sectors that leverages the Chocolatey Windows package manager to deliver a backdoor called Serpent on compromised systems. Enterprise security firm Proofpoint attributed the attacks to a likely advanced threat actor based on the tactics and the victimology patterns observed. The ultimate objective of the campaign remains presently unknown. "The threat actor attempted to install a backdoor on a potential victim's device, which could enable remote administration, command and control (C2), data theft, or deliver other additional payloads," Proofpoint researchers said in a report shared with The Hacker News.  The phishing lure that triggers the infection sequence makes use of a resume-themed subject line, with the attached macro-embedded Microsoft Word document masquerading as information related to the European Union's General Data Protection Regulation (GDPR). Enabling the macros results in its execution, which retrieves a seemingly harmless image file hosted on a remote server but actually contains a Base64-encoded PowerShell script that's obscured using steganography, a little-used method of concealing malicious code within an image or audio in order to circumvent detection.  The PowerShell script, in turn, is engineered to install the Chocolatey utility on the Windows machine, which is then utilized to install the Python package installer pip, the latter of which acts as conduit to install the PySocks proxy library. Also retrieved by the same PowerShell script is another image file from the same remote server that includes the camouflaged Python backdoor dubbed Serpent, which comes with capabilities to execute commands transmitted from the C2 server.  In addition to steganography, the use of widely recognized tools such as Chocolatey as an initial payload for follow-on deployment of genuine Python packages is an attempt to stay under the radar and not be flagged as a threat, Proofpoint said. The attacks have not unearthed associations with a previously identified actor or group, but are suspected to be the work of a sophisticated hacking crew. "This is a novel application of a variety of technologies that are often legitimately used within organizations," Sherrod DeGrippo, vice president of threat research and detection at Proofpoint, said in a statement. "It capitalizes on many organizations', specifically technical groups, desire to allow their users to be 'self-sufficient' in regards to self-tooling and package managers. Additionally, the use of steganography is unusual and something we don't see regularly."   Found this article interesting? Follow THN on Facebook, Twitter  and LinkedIn to read more exclusive content we post. | Các nhà nghiên cứu đã tiết lộ một chiến dịch email nhắm mục tiêu mới nhằm vào các tổ chức của Pháp trong lĩnh vực xây dựng, bất động sản và chính phủ, thúc đẩy trình quản lý gói Chocolatey Windows cung cấp một cửa sau có tên Serpent trên các hệ thống bị xâm phạm. Công ty bảo mật doanh nghiệp Proofpoint quy các cuộc tấn công là do một tác nhân có khả năng xảy ra mối đe dọa nâng cao dựa trên các chiến thuật và mô hình nạn nhân được quan sát thấy. Mục tiêu cuối cùng của chiến dịch hiện vẫn chưa được biết. Các nhà nghiên cứu của Proofpoint cho biết trong một báo cáo được chia sẻ với The Hacker News: "Kẻ đe dọa đã cố gắng cài đặt một cửa hậu trên thiết bị của nạn nhân tiềm năng, có thể cho phép quản trị, ra lệnh và điều khiển từ xa (C2), đánh cắp dữ liệu hoặc cung cấp các tải trọng bổ sung khác".  Lời dụ dỗ lừa đảo kích hoạt chuỗi lây nhiễm sử dụng dòng tiêu đề có chủ đề sơ yếu lý lịch, với tài liệu Microsoft Word nhúng macro đính kèm giả mạo thành thông tin liên quan đến Quy định chung về bảo vệ dữ liệu của Liên minh Châu Âu (GDPR). Việc bật macro dẫn đến việc thực thi nó, truy xuất tệp hình ảnh có vẻ vô hại được lưu trữ trên máy chủ từ xa nhưng thực sự chứa tập lệnh PowerShell được mã hóa Base64 bị che khuất bằng cách sử dụng mật mã, một phương pháp ít được sử dụng để che giấu mã độc hại trong hình ảnh hoặc âm thanh theo thứ tự để vượt qua sự phát hiện.  Đến lượt mình, tập lệnh PowerShell được thiết kế để cài đặt tiện ích Chocolatey trên máy Windows, sau đó được sử dụng để cài đặt pip trình cài đặt gói Python, sau đó nó hoạt động như một đường dẫn để cài đặt thư viện proxy PySocks. Cũng được truy xuất bởi cùng một tập lệnh PowerShell là một tệp hình ảnh khác từ cùng một máy chủ từ xa bao gồm cửa hậu Python ngụy trang có tên Serpent, đi kèm với khả năng thực thi các lệnh được truyền từ máy chủ C2.  Ngoài việc sử dụng steganography, việc sử dụng các công cụ được công nhận rộng rãi như Chocolatey làm trọng tải ban đầu để tiếp tục triển khai các gói Python chính hãng là một nỗ lực để duy trì tầm ngắm và không bị gắn cờ là mối đe dọa, Proofpoint cho biết. Các cuộc tấn công không phát hiện ra mối liên hệ với một tác nhân hoặc nhóm đã được xác định trước đó, nhưng bị nghi ngờ là hoạt động của một nhóm tấn công tinh vi. "Đây là một ứng dụng mới của nhiều loại công nghệ thường được sử dụng hợp pháp trong các tổ chức", Sherrod DeGrippo, phó chủ tịch nghiên cứu và phát hiện mối đe dọa tại Proofpoint, cho biết trong một tuyên bố. "Nó tận dụng lợi thế của nhiều tổ chức, cụ thể là các nhóm kỹ thuật, mong muốn cho phép người dùng của họ 'tự cung tự cấp' liên quan đến việc tự cung cấp công cụ và quản lý gói. Ngoài ra, việc sử dụng steganography là điều bất thường và chúng tôi không thấy thường xuyên . "   Tìm thấy bài viết này thú vị? Theo dõi THN trên Facebook, Twitter  và LinkedIn để đọc thêm nội dung độc quyền mà chúng tôi đăng. |

# 'CryptoRom' Crypto Scam Abusing iPhone Features to Target Mobile Users

📅Date: March 21, 2022 👤Author: Ravie Lakshmanan

Link tham khảo: *https://thehackernews.com/2022/03/cryptorom-crypto-scam-abusing-iphone.html*



|  |  |
| --- | --- |
| Title: 🐄'CryptoRom' Crypto Scam Abusing iPhone Features to Target Mobile Users | Title: 🐄'CryptoRom' Lừa đảo tiền điện tử Lạm dụng các tính năng của iPhone để nhắm mục tiêu người dùng di động |
| Social engineering attacks leveraging a combination of romantic lures and cryptocurrency fraud have been deceiving unsuspecting victims into installing fake apps by taking advantage of legitimate iOS features like TestFlight and Web Clips. Cybersecurity company Sophos, which has named the organized crime campaign "CryptoRom," characterized it as a wide-ranging global scam. "This style of cyber-fraud, known as sha zhu pan (杀猪盘) — literally 'pig butchering plate' — is a well-organized, syndicated scam operation that uses a combination of often romance-centered social engineering and fraudulent financial applications and websites to ensnare victims and steal their savings after gaining their confidence," Sophos analyst Jagadeesh Chandraiah said in a report published last week.  The campaign works by approaching potential targets through dating apps like Bumble, Tinder, Facebook Dating, and Grindr, before moving the conversation to messaging apps such as WhatsApp and urging the victims to install a cryptocurrency trading application that's designed to mimic popular brands and lock people out of their accounts and freeze their funds.  Previous variants of the social engineering scam observed in October 2021 were found to leverage lookalike App Store pages to deceive people into installing the rogue iOS apps, not to mention abuse Apple's Developer Enterprise Program to deploy sketchy mobile provisioning profiles to distribute the malware.  But the new attack wave observed by Sophos takes advantage of Apple's TestFlight beta testing framework and a device management feature called Web Clips, which allows URLs to specific web pages to be placed on the home screen of users' iOS devices just like a traditional application.  Once installed, the crooks promise the individuals huge financial returns in return for making a monetary investment, while artificially manipulating the numbers on the fake app to "reinforce the con" and convince the victims into believing that "they are making money" through the platform. "The scam doesn't end with just fooling victims into investing," Chandraiah elaborated. "When victims try to withdraw funds from their big 'profit,' the crooks use the app to inform them that they need to pay a 'tax' of 20% of their profits before funds can be withdrawn — and threaten that all their investments will be confiscated by tax authorities if they do not pay."   Found this article interesting? Follow THN on Facebook, Twitter  and LinkedIn to read more exclusive content we post. | Các cuộc tấn công kỹ thuật xã hội tận dụng sự kết hợp của những chiêu dụ lãng mạn và gian lận tiền điện tử đã đánh lừa những nạn nhân không nghi ngờ cài đặt các ứng dụng giả bằng cách tận dụng các tính năng hợp pháp của iOS như TestFlight và Web Clips. Công ty an ninh mạng Sophos, đã đặt tên cho chiến dịch tội phạm có tổ chức là "CryptoRom", đã mô tả nó là một trò lừa đảo trên phạm vi toàn cầu. "Phong cách lừa đảo mạng này, được gọi là sha zhu pan (杀猪 盘) - nghĩa đen là 'đĩa thịt lợn' - là một hoạt động lừa đảo được tổ chức tốt, sử dụng sự kết hợp của kỹ thuật xã hội thường lấy sự lãng mạn làm trung tâm và các ứng dụng tài chính gian lận và các trang web để gài bẫy nạn nhân và ăn cắp tiền tiết kiệm của họ sau khi đã có được niềm tin của họ ", nhà phân tích Jagadeesh Chandraiah của Sophos cho biết trong một báo cáo được công bố vào tuần trước.  Chiến dịch hoạt động bằng cách tiếp cận các mục tiêu tiềm năng thông qua các ứng dụng hẹn hò như Bumble, Tinder, Facebook Dating và Grindr, trước khi chuyển cuộc trò chuyện sang các ứng dụng nhắn tin như WhatsApp và kêu gọi nạn nhân cài đặt ứng dụng giao dịch tiền điện tử được thiết kế để bắt chước các thương hiệu nổi tiếng và khóa mọi người ra khỏi tài khoản của họ và đóng băng tiền của họ.  Các biến thể trước đây của trò lừa đảo kỹ thuật xã hội được quan sát vào tháng 10 năm 2021 đã được phát hiện là tận dụng các trang App Store trông giống hệt để đánh lừa mọi người cài đặt các ứng dụng iOS giả mạo, chưa kể đến việc lạm dụng Chương trình Doanh nghiệp dành cho nhà phát triển của Apple để triển khai các hồ sơ cấp phép di động sơ sài nhằm phát tán phần mềm độc hại.  Nhưng làn sóng tấn công mới mà Sophos quan sát được lợi dụng khung thử nghiệm TestFlight beta của Apple và một tính năng quản lý thiết bị có tên là Web Clips, cho phép đặt URL đến các trang web cụ thể trên màn hình chính của thiết bị iOS của người dùng giống như một ứng dụng truyền thống.  Sau khi cài đặt, kẻ gian hứa với các cá nhân lợi nhuận tài chính khổng lồ để đổi lại việc đầu tư tiền tệ, trong khi thao túng giả tạo các con số trên ứng dụng giả mạo để "củng cố kẻ lừa đảo" và thuyết phục nạn nhân tin rằng "họ đang kiếm tiền" thông qua nền tảng . Chandraiah giải thích thêm: “Trò lừa đảo không kết thúc bằng việc lừa nạn nhân đầu tư. "Khi nạn nhân cố gắng rút tiền từ 'lợi nhuận' lớn của họ, kẻ gian sử dụng ứng dụng để thông báo rằng họ cần phải trả 'thuế' 20% lợi nhuận trước khi tiền có thể được rút - và đe dọa rằng tất cả các khoản đầu tư của họ sẽ bị cơ quan thuế tịch thu nếu không nộp ”.   Tìm thấy bài viết này thú vị? Theo dõi THN trên Facebook, Twitter  và LinkedIn để đọc thêm nội dung độc quyền mà chúng tôi đăng. |

# South Korean DarkHotel Hackers Targeted Luxury Hotels in Macau

📅Date: March 21, 2022 👤Author: Ravie Lakshmanan

Link tham khảo: *https://thehackernews.com/2022/03/south-korean-darkhotel-hackers-targeted.html*



|  |  |
| --- | --- |
| Title: 🐄South Korean DarkHotel Hackers Targeted Luxury Hotels in Macau | Title: 🐄Tin tặc DarkHotel của Hàn Quốc đã nhắm mục tiêu vào các khách sạn sang trọng ở Ma Cao |
| Luxury hotels in the Chinese special administrative region of Macau were the target of a malicious spear-phishing campaign from the second half of November 2021 and through mid-January 2022. Cybersecurity firm Trellix attributed the campaign with moderate confidence to a suspected South Korean advanced persistent threat (APT) tracked as DarkHotel, building on research previously published by Zscaler in December 2021. Believed to be active since 2007, DarkHotel has a history of striking "senior business executives by uploading malicious code to their computers through infiltrated hotel Wi-Fi networks, as well as through spear-phishing and P2P attacks," Zscaler researchers Sahil Antil and Sudeep Singh said. Prominent sectors targeted include law enforcement, pharmaceuticals, and automotive manufacturers.  The attack chains involved distributing email messages directed to individuals in executive roles in the hotel, such as the vice president of human resources, assistant manager, and front office manager, indicating that the intrusions were aimed at staff who were in possession of access to the hotel's network. In one phishing lure sent to 17 different hotels on December 7, the email purported to be from the Macau Government Tourism Office and urged the victims to open an Excel file named "信息.xls" ("information.xls"). In another case, the emails were faked to gather details about people staying in the hotels.  The malware-laced Microsoft Excel file, when opened, tricked the recipients into enabling macros, triggering an exploit chain to gather and exfiltrate sensitive data from the compromised machines back to a remote command-and-control (C2) server ("fsm-gov[.]com") that impersonated the government website for the Federated States of Micronesia (FSM). "This IP was used by the actor to drop new payloads as first stages to set up the victim environment for system information exfiltration and potential next steps," Trellix researchers Thibault Seret and John Fokker said in a report published last week. "Those payloads were used to target major hotel chains in Macau, including the Grand Coloane Resort and Wynn Palace."  Also noteworthy is the fact that the C2 server IP address has continued to remain active despite prior public disclosure and that it's being used to serve phishing pages for an unrelated credential harvesting attack directed at MetaMask cryptocurrency wallet users. The campaign is said to have to met its inevitable end on January 18, 2022 coinciding with the rise of COVID-19 cases in Macau, prompting the cancelation or postponement of a number of international trade conferences that were set to take place in the targeted hotels. "The group was trying to lay the foundation for a future campaign involving these specific hotels," the researchers said. "In this campaign, the COVID-19 restrictions threw a wrench in the threat actor's engine, but that doesn't mean they have abandoned this approach."   Found this article interesting? Follow THN on Facebook, Twitter  and LinkedIn to read more exclusive content we post. | Các khách sạn sang trọng ở khu hành chính đặc biệt Ma Cao của Trung Quốc là mục tiêu của một chiến dịch lừa đảo ác ý từ nửa cuối tháng 11 năm 2021 và đến giữa tháng 1 năm 2022. Công ty an ninh mạng Trellix quy kết chiến dịch với độ tin cậy vừa phải là do một mối đe dọa dai dẳng tiên tiến (APT) bị nghi ngờ của Hàn Quốc được theo dõi là DarkHotel, dựa trên nghiên cứu được Zscaler công bố trước đó vào tháng 12 năm 2021. Được cho là hoạt động từ năm 2007, DarkHotel có lịch sử gây ấn tượng với "các giám đốc kinh doanh cấp cao bằng cách tải mã độc lên máy tính của họ thông qua mạng Wi-Fi của khách sạn bị xâm nhập, cũng như thông qua các cuộc tấn công lừa đảo trực tuyến và P2P", các nhà nghiên cứu của Zscaler là Sahil Antil và Sudeep Singh nói. Các lĩnh vực nổi bật được nhắm mục tiêu bao gồm thực thi pháp luật, dược phẩm và nhà sản xuất ô tô.  Các chuỗi tấn công liên quan đến việc phân phát các thông điệp email trực tiếp đến các cá nhân có vai trò điều hành trong khách sạn, chẳng hạn như phó chủ tịch bộ phận nhân sự, trợ lý giám đốc và giám đốc văn phòng, cho thấy rằng các cuộc xâm nhập nhằm vào nhân viên có quyền truy cập vào mạng của khách sạn. Trong một lời dụ dỗ lừa đảo được gửi đến 17 khách sạn khác nhau vào ngày 7 tháng 12, email được cho là từ Văn phòng Du lịch Chính phủ Ma Cao và kêu gọi các nạn nhân mở một tệp Excel có tên "信息 .xls" ("information.xls"). Trong một trường hợp khác, các email được làm giả để thu thập thông tin chi tiết về những người ở trong khách sạn.  Tệp Microsoft Excel chứa phần mềm độc hại, khi được mở, đã đánh lừa người nhận bật macro, kích hoạt chuỗi khai thác để thu thập và lấy dữ liệu nhạy cảm từ các máy bị xâm nhập trở lại máy chủ điều khiển và kiểm soát từ xa (C2) ("fsm-gov [.] com ") đã mạo danh trang web của chính phủ cho Liên bang Micronesia (FSM). Các nhà nghiên cứu của Trellix, Thibault Seret và John Fokker cho biết trong một báo cáo được công bố vào tuần trước: “IP này đã được tác nhân sử dụng để giảm tải trọng mới như là giai đoạn đầu tiên nhằm thiết lập môi trường nạn nhân cho quá trình lọc thông tin hệ thống và các bước tiếp theo tiềm năng”. "Những trọng tải đó được sử dụng để nhắm vào các chuỗi khách sạn lớn ở Ma Cao, bao gồm cả Grand Coloane Resort và Wynn Palace."  Cũng đáng chú ý là thực tế là địa chỉ IP của máy chủ C2 vẫn tiếp tục hoạt động mặc dù đã được tiết lộ công khai trước đó và nó được sử dụng để phục vụ các trang lừa đảo cho một cuộc tấn công thu thập thông tin xác thực không liên quan nhắm vào người dùng ví tiền điện tử MetaMask. Chiến dịch được cho là sẽ phải kết thúc không thể tránh khỏi vào ngày 18 tháng 1 năm 2022 trùng với sự gia tăng của các trường hợp COVID-19 ở Ma Cao, khiến một số hội nghị thương mại quốc tế được định tổ chức tại các khách sạn mục tiêu phải hủy bỏ hoặc hoãn lại. . Các nhà nghiên cứu cho biết: “Nhóm đang cố gắng tạo nền tảng cho một chiến dịch trong tương lai liên quan đến những khách sạn cụ thể này. "Trong chiến dịch này, các hạn chế COVID-19 đã ném một chìa khóa vào động cơ của kẻ đe dọa, nhưng điều đó không có nghĩa là họ đã từ bỏ cách tiếp cận này."   Tìm thấy bài viết này thú vị? Theo dõi THN trên Facebook, Twitter  và LinkedIn để đọc thêm nội dung độc quyền mà chúng tôi đăng. |

# Hackers Target Bank Networks with new Rootkit to Steal Money from ATM Machines

📅Date: March 18, 2022 👤Author: Ravie Lakshmanan

Link tham khảo: *https://thehackernews.com/2022/03/hackers-target-bank-networks-with-new.html*



|  |  |
| --- | --- |
| Title: 🐄Hackers Target Bank Networks with new Rootkit to Steal Money from ATM Machines | Title: 🐄Tin tặc Nhắm mục tiêu mạng ngân hàng với Rootkit mới để ăn cắp tiền từ máy ATM |
| A financially motivated threat actor has been observed deploying a previously unknown rootkit targeting Oracle Solaris systems with the goal of compromising Automatic Teller Machine (ATM) switching networks and carrying out unauthorized cash withdrawals at different banks using fraudulent cards. Threat intelligence and incident response firm Mandiant is tracking the cluster under the moniker UNC2891, with some of the group's tactics, techniques, and procedures sharing overlaps with that of another cluster dubbed UNC1945. The intrusions staged by the actor involve "a high degree of OPSEC and leverage both public and private malware, utilities, and scripts to remove evidence and hinder response efforts," Mandiant researchers said in a new report published this week.  Even more concerningly, the attacks spanned several years in some cases, during the entirety of which the actor remained undetected by taking advantage of a rootkit called CAKETAP, whic is designed to conceal network connections, processes, and files. Mandiant, which was able to recover memory forensic data from one of the victimized ATM switch servers, noted that one variant of the kernel rootkit came with specialized features that enabled it to intercept card and PIN verification messages and use the stolen data to perform fraudulent cash withdrawals from ATM terminals.  Also put to use are two backdoors known as SLAPSTICK and TINYSHELL, both attributed to UNC1945 and are employed to gain persistent remote access to mission-critical systems as well as shell execution and file transfers via rlogin, telnet, or SSH. "In line with the group's familiarity with Unix and Linux based systems, UNC2891 often named and configured their TINYSHELL backdoors with values that masqueraded as legitimate services that might be overlooked by investigators, such as systemd (SYSTEMD), name service cache daemon (NCSD), and the Linux at daemon (ATD)," the researchers pointed out.  Additionally, the attack chains were spotted utilizing a variety of malware and publicly-available utilities, including –  STEELHOUND – A variant of the STEELCORGI in-memory dropper that's used to decrypt an embedded payload and encrypt new binaries WINGHOOK – A keylogger for Linux and Unix based operating systems that captures the data in an encoded format WINGCRACK – A utility that's used to parse the encoded content generated by WINGHOOK WIPERIGHT – An ELF utility that erases log entries pertaining to a specific user on Linux and Unix based systems MIGLOGCLEANER – An ELF utility that wipes logs or remove certain strings from logs on Linux and Unix based systems  "[UNC2891] uses their skill and experience to take full advantage of the decreased visibility and security measures that are often present in Unix and Linux environments," the researchers said. "While some of the overlaps between UNC2891 and UNC1945 are notable, it is not conclusive enough to attribute the intrusions to a single threat group."   Found this article interesting? Follow THN on Facebook, Twitter  and LinkedIn to read more exclusive content we post. | Một kẻ đe dọa có động cơ tài chính đã được quan sát thấy đã triển khai một rootkit trước đây chưa được biết đến nhằm vào các hệ thống Oracle Solaris với mục tiêu xâm phạm mạng chuyển mạch Máy rút tiền tự động (ATM) và thực hiện rút tiền trái phép tại các ngân hàng khác nhau bằng thẻ gian lận. Công ty ứng phó sự cố và tình báo mối đe dọa Mandiant đang theo dõi cụm này với biệt danh UNC2891, với một số chiến thuật, kỹ thuật và thủ tục của nhóm này trùng lặp với cụm khác có tên UNC1945. Các nhà nghiên cứu Mandiant cho biết trong một báo cáo mới được công bố trong tuần này, các cuộc xâm nhập do kẻ này dàn dựng liên quan đến "mức độ cao của OPSEC và tận dụng cả phần mềm độc hại, tiện ích và tập lệnh công khai và riêng tư để xóa bằng chứng và cản trở nỗ lực phản ứng".  Đáng quan tâm hơn, các cuộc tấn công kéo dài vài năm trong một số trường hợp, trong suốt thời gian mà tác nhân vẫn không bị phát hiện bằng cách lợi dụng bộ rootkit có tên là CAKETAP, được thiết kế để che giấu các kết nối mạng, quy trình và tệp. Mandiant, công ty có khả năng khôi phục dữ liệu pháp y trong bộ nhớ từ một trong những máy chủ chuyển mạch ATM bị nạn, lưu ý rằng một biến thể của bộ rootkit nhân đi kèm với các tính năng chuyên biệt cho phép nó đánh chặn thông báo xác minh thẻ và mã PIN và sử dụng dữ liệu bị đánh cắp để thực hiện hành vi gian lận tiền mặt. rút tiền từ các thiết bị đầu cuối ATM.  Cũng được đưa vào sử dụng là hai backdoor được gọi là SLAPSTICK và TINYSHELL, cả hai đều được gán cho UNC1945 và được sử dụng để có được quyền truy cập từ xa liên tục vào các hệ thống quan trọng cũng như thực thi shell và truyền tệp qua rlogin, telnet hoặc SSH. "Do sự quen thuộc của nhóm với các hệ thống dựa trên Unix và Linux, UNC2891 thường đặt tên và định cấu hình các cửa hậu TINYSHELL của họ bằng các giá trị giả mạo là các dịch vụ hợp pháp mà các nhà điều tra có thể bỏ qua, chẳng hạn như systemd (SYSTEMD), daemon bộ đệm tên dịch vụ (NCSD) và Linux tại daemon (ATD), "các nhà nghiên cứu chỉ ra.  Ngoài ra, các chuỗi tấn công được phát hiện sử dụng nhiều phần mềm độc hại và các tiện ích công khai, bao gồm -  STEELHOUND - Một biến thể của ống nhỏ giọt trong bộ nhớ STEELCORGI được sử dụng để giải mã tải trọng được nhúng và mã hóa các tệp nhị phân mới WINGHOOK - Một keylogger cho các hệ điều hành dựa trên Linux và Unix để ghi lại dữ liệu ở định dạng được mã hóa WINGCRACK - Một tiện ích được sử dụng để phân tích cú pháp nội dung được mã hóa được tạo bởi WINGHOOK WIPERIGHT - Một tiện ích ELF xóa các mục nhật ký liên quan đến một người dùng cụ thể trên các hệ thống dựa trên Linux và Unix MIGLOGCLEANER - Một tiện ích ELF xóa sạch nhật ký hoặc xóa một số chuỗi nhất định khỏi nhật ký trên các hệ thống dựa trên Linux và Unix  Các nhà nghiên cứu cho biết: "[UNC2891] sử dụng kỹ năng và kinh nghiệm của họ để tận dụng tối đa khả năng hiển thị và các biện pháp bảo mật giảm thường có trong môi trường Unix và Linux". "Mặc dù một số điểm trùng lặp giữa UNC2891 và UNC1945 là đáng chú ý, nhưng vẫn chưa đủ kết luận để quy các vụ xâm nhập vào một nhóm mối đe dọa duy nhất."   Tìm thấy bài viết này thú vị? Theo dõi THN trên Facebook, Twitter  và LinkedIn để đọc thêm nội dung độc quyền mà chúng tôi đăng. |

# Experts Find Some Affiliates of BlackMatter Now Spreading BlackCat Ransomware

📅Date: March 18, 2022 👤Author: Ravie Lakshmanan

Link tham khảo: *https://thehackernews.com/2022/03/experts-find-some-affiliates-of.html*



|  |  |
| --- | --- |
| Title: 🐄Experts Find Some Affiliates of BlackMatter Now Spreading BlackCat Ransomware | Title: 🐄Các chuyên gia tìm thấy một số chi nhánh của BlackMatter hiện đang phát tán phần mềm ransomware BlackCat |
| An analysis of two ransomware attacks has identified overlaps in the tactics, techniques, and procedures (TTPs) between BlackCat and BlackMatter, indicating a strong connection between the two groups. While it's typical of ransomware groups to rebrand their operations in response to increased visibility into their attacks, BlackCat (aka Alphv) marks a new frontier in that the cyber crime cartel is built out of affiliates of other ransomware-as-a-service (RaaS) operations. BlackCat first emerged in November 2021 and has since targeted several organizations worldwide over the past few months. It has been called out for being similar to BlackMatter, a short-lived ransomware family that originated from DarkSide, which, in turn, attracted notoriety for its high-profile attack on Colonial Pipeline in May 2021.  In an interview with Recorded Future's The Record last month, a BlackCat representative dismissed speculations that it's a rebranding of BlackMatter, while noting that it's made up of affiliates associated with other RaaS groups.  "In part, we are all connected to gandrevil [GandCrab / REvil], blackside [BlackMatter / DarkSide], mazegreggor [Maze / Egregor], lockbit, etc., because we are adverts (aka affiliates)," the unnamed representative was quoted as saying. "We borrowed their advantages and eliminated their disadvantages."  "BlackCat seems to be a case of vertical business expansion," Cisco Talos researchers Tiago Pereira and Caitlin Huey said. "In essence, it's a way to control the upstream supply chain by making a service that is key to their business (the RaaS operator) better suited for their needs and adding another source of revenue." What's more, the cybersecurity firm said it observed a number of commonalities between a BlackMatter attack in September 2021 and that of a BlackCat attack from December 2021, including the tools and the file names used as well as a domain employed to maintain persistent access to the target network. This overlapping use of the same command-and-control address has raised the possibility that the affiliate that used BlackMatter was likely one of the early adopters of BlackCat, with both the attacks taking more than 15 days to reach the encryption stage.  "As we have seen several times before, RaaS services come and go. Their affiliates, however, are likely to simply move on to a new service. And with them, many of the TTPs are likely to persist," the researchers said. The findings come as BlackBerry detailed a new .NET-based ransomware family called LokiLocker that not only encrypts the files but also incorporates an optional wiper functionality that's designed to erase all non-system files and overwrite the master boot record (MBR) should a victim refuse to pay up within a specified timeframe. "LokiLocker works as a limited-access ransomware-as-a-service scheme that appears to be sold to a relatively small number of carefully vetted affiliates behind closed doors," the researchers said. Active since at least August 2021, a majority of victims detected so far are concentrated in Eastern Europe and Asia.   Found this article interesting? Follow THN on Facebook, Twitter  and LinkedIn to read more exclusive content we post. | Một phân tích về hai cuộc tấn công ransomware đã xác định được sự chồng chéo về chiến thuật, kỹ thuật và quy trình (TTP) giữa BlackCat và BlackMatter, cho thấy mối liên hệ chặt chẽ giữa hai nhóm. Trong khi các nhóm ransomware là điển hình của việc đổi thương hiệu hoạt động của họ để đáp ứng với việc tăng khả năng hiển thị trước các cuộc tấn công của họ, BlackCat (hay còn gọi là Alphv) đánh dấu một biên giới mới trong đó tập đoàn tội phạm mạng được xây dựng từ các chi nhánh của dịch vụ ransomware khác (RaaS ) hoạt động. BlackCat xuất hiện lần đầu tiên vào tháng 11 năm 2021 và kể từ đó đã nhắm mục tiêu đến một số tổ chức trên toàn thế giới trong vài tháng qua. Nó đã được gọi là tương tự như BlackMatter, một họ ransomware tồn tại trong thời gian ngắn có nguồn gốc từ DarkSide, đến lượt nó, thu hút tai tiếng vì cuộc tấn công nổi tiếng vào Colonial Pipeline vào tháng 5 năm 2021.  Trong một cuộc phỏng vấn với The Record của Recorded Future vào tháng trước, đại diện của BlackCat đã bác bỏ những suy đoán rằng đó là thương hiệu của BlackMatter, đồng thời lưu ý rằng nó được tạo thành từ các chi nhánh liên kết với các nhóm RaaS khác.  "Một phần, tất cả chúng ta đều kết nối với gandrevil [GandCrab / REvil], blackside [BlackMatter / DarkSide], mazegreggor [Maze / Egregor], lockbit, v.v., bởi vì chúng tôi là nhà quảng cáo (hay còn gọi là chi nhánh)", đại diện giấu tên được trích dẫn như đang nói. "Chúng tôi mượn lợi thế của họ và loại bỏ nhược điểm của họ."  Các nhà nghiên cứu Tiago Pereira và Caitlin Huey của Cisco Talos cho biết: “BlackCat dường như là một trường hợp mở rộng kinh doanh theo chiều dọc. "Về bản chất, đó là một cách để kiểm soát chuỗi cung ứng thượng nguồn bằng cách tạo ra một dịch vụ then chốt đối với hoạt động kinh doanh của họ (nhà điều hành RaaS) phù hợp hơn với nhu cầu của họ và thêm một nguồn doanh thu khác." Hơn nữa, công ty an ninh mạng cho biết họ đã quan sát thấy một số điểm tương đồng giữa cuộc tấn công BlackMatter vào tháng 9 năm 2021 và cuộc tấn công BlackCat từ tháng 12 năm 2021, bao gồm các công cụ và tên tệp được sử dụng cũng như miền được sử dụng để duy trì quyền truy cập liên tục vào mạng mục tiêu. Việc sử dụng chồng chéo cùng một địa chỉ lệnh và điều khiển đã làm tăng khả năng đơn vị liên kết đã sử dụng BlackMatter có thể là một trong những người chấp nhận BlackCat sớm nhất, với cả hai cuộc tấn công đều mất hơn 15 ngày để đạt được giai đoạn mã hóa.  "Như chúng ta đã thấy nhiều lần trước đây, các dịch vụ RaaS đến và đi. Tuy nhiên, các chi nhánh của họ có khả năng chỉ chuyển sang một dịch vụ mới. Và cùng với họ, nhiều TTP có khả năng tồn tại", các nhà nghiên cứu cho biết. Phát hiện được đưa ra khi BlackBerry trình bày chi tiết về một họ ransomware dựa trên .NET mới có tên là LokiLocker không chỉ mã hóa các tệp mà còn kết hợp chức năng xóa tùy chọn được thiết kế để xóa tất cả các tệp không thuộc hệ thống và ghi đè lên bản ghi khởi động chính (MBR) nếu là nạn nhân. từ chối thanh toán trong một khung thời gian cụ thể. Các nhà nghiên cứu cho biết: “LokiLocker hoạt động như một chương trình ransomware-as-a-service có quyền truy cập hạn chế, dường như được bán cho một số lượng tương đối nhỏ các chi nhánh đã được kiểm tra cẩn thận đằng sau những cánh cửa đóng kín”. Hoạt động ít nhất từ ​​tháng 8 năm 2021, phần lớn nạn nhân được phát hiện cho đến nay tập trung ở Đông Âu và Châu Á.   Tìm thấy bài viết này thú vị? Theo dõi THN trên Facebook, Twitter  và LinkedIn để đọc thêm nội dung độc quyền mà chúng tôi đăng. |

# Google Uncovers 'Initial Access Broker' Working with Conti Ransomware Gang

📅Date: March 18, 2022 👤Author: Ravie Lakshmanan

Link tham khảo: *https://thehackernews.com/2022/03/google-uncovers-initial-access-broker.html*

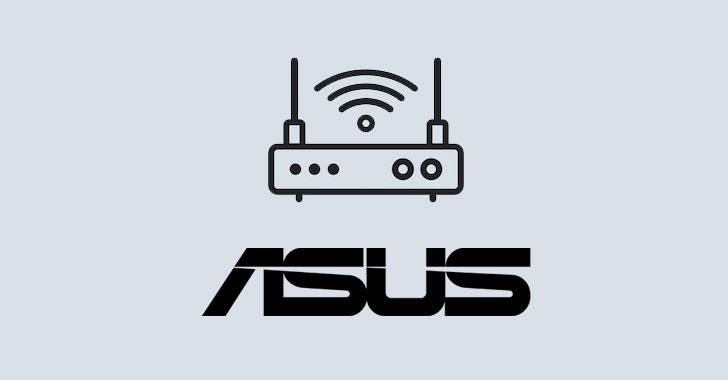


|  |  |
| --- | --- |
| Title: 🐄Google Uncovers 'Initial Access Broker' Working with Conti Ransomware Gang | Title: 🐄Google cho thấy 'Nhà môi giới truy cập ban đầu' làm việc với Conti Ransomware Gang |
| Google's Threat Analysis Group (TAG) took the wraps off a new initial access broker that it said is closely affiliated to a Russian cyber crime gang notorious for its Conti and Diavol ransomware operations. Dubbed Exotic Lily, the financially motivated threat actor has been observed exploiting a now-patched critical flaw in the Microsoft Windows MSHTML platform (CVE-2021-40444) as part of widespread phishing campaigns that involved sending no fewer than 5,000 business proposal-themed emails a day to 650 targeted organizations globally. "Initial access brokers are the opportunistic locksmiths of the security world, and it's a full-time job," TAG researchers Vlad Stolyarov and Vlad Stolyarov said. "These groups specialize in breaching a target in order to open the doors — or the Windows — to the malicious actor with the highest bid."  Exotic Lily, first spotted in September 2021, is said to have been involved in data exfiltration and deployment of the human-operated Conti and Diavol ransomware strains, both of which share overlaps with Wizard Spider, the Russian cyber criminal syndicate that's also known for operating TrickBot, BazarBackdoor, and Anchor. "Yes, this is a possibility, especially considering this is more sophisticated and targeted than a traditional spam campaign, but we don't know for sure as of now," Google TAG told The Hacker News when asked whether Exotic Lily could be another extension of the Wizard Spider group. "In the Conti leaks, Conti members mention 'spammers' as someone who they work with (e.g., provide custom-built 'crypted' malware samples, etc.) through outsourcing. However, most of the 'spammers' don't seem to be present (or actively communicate) in the chat, hence leading to a conclusion they're operating as a separate entity."  The threat actor's social engineering lures, sent from spoofed email accounts, have specifically singled out IT, cybersecurity, and healthcare sectors, although post November 2021, the attacks have grown to be more indiscriminate, targeting a wide variety of organizations and industries. Besides using fictitious companies and identities as a means to build trust with the targeted entities, Exotic Lily has leveraged legitimate file-sharing services like WeTransfer, TransferNow and OneDrive to deliver BazarBackdoor payloads in a bid to evade detection mechanisms.  The rogue personas often posed as employees of firms such as Amazon, complete with fraudulent social media profiles on LinkedIn that featured fake AI-generated profile pictures. The group is also said to have impersonated real company employees by lifting their personal data from social media and business databases like RocketReach and CrunchBase.  "At the final stage, the attacker would upload the payload to a public file-sharing service (TransferNow, TransferXL, WeTransfer or OneDrive) and then use a built-in email notification feature to share the file with the target, allowing the final email to originate from the email address of a legitimate file-sharing service and not the attacker's email, which presents additional detection challenges," the researchers said. Also delivered using the MHTML exploit is a custom loader called Bumblebee that's orchestrated to gather and exfiltrate system information to a remote server, which responds back commands to execute shellcode and run next-stage executables, including Cobalt Strike. An analysis of the Exotic Lily's communication activity indicates that the threat actors have a "typical 9-to-5 job" on weekdays and may be possibly working from a Central or an Eastern Europe time zone. "Exotic Lily seems to operate as a separate entity, focusing on acquiring initial access through email campaigns, with follow-up activities that include deployment of Conti and Diavol ransomware, which are performed by a different set of actors," the researchers concluded.   Found this article interesting? Follow THN on Facebook, Twitter  and LinkedIn to read more exclusive content we post. | Nhóm phân tích mối đe dọa của Google (TAG) đã kết thúc tốt đẹp với một nhà môi giới truy cập ban đầu mới mà họ cho là có liên kết chặt chẽ với một băng nhóm tội phạm mạng của Nga nổi tiếng với các hoạt động ransomware Conti và Diavol. Được mệnh danh là Exotic Lily, kẻ đe dọa có động cơ tài chính đã được quan sát khai thác một lỗ hổng nghiêm trọng hiện đã được vá trong nền tảng Microsoft Windows MSHTML (CVE-2021-40444) như một phần của các chiến dịch lừa đảo lan rộng liên quan đến việc gửi không dưới 5.000 email theo chủ đề đề xuất kinh doanh một ngày cho 650 tổ chức được nhắm mục tiêu trên toàn cầu. "Các nhà môi giới truy cập ban đầu là những thợ khóa cơ hội của thế giới an ninh và đó là công việc toàn thời gian", các nhà nghiên cứu Vlad Stolyarov và Vlad Stolyarov của TAG cho biết. "Các nhóm này chuyên xâm phạm mục tiêu để mở cửa - hoặc Windows - cho kẻ độc hại với giá thầu cao nhất."  Exotic Lily, được phát hiện lần đầu tiên vào tháng 9 năm 2021, được cho là đã tham gia vào quá trình lọc và triển khai dữ liệu của các chủng ransomware Conti và Diavol do con người điều hành, cả hai đều trùng lặp với Wizard Spider, tổ chức tội phạm mạng của Nga cũng được biết đến để vận hành TrickBot, BazarBackdoor và Anchor. "Đúng, đây là một khả năng, đặc biệt là khi xem xét điều này phức tạp hơn và được nhắm mục tiêu hơn so với một chiến dịch spam truyền thống, nhưng chúng tôi không biết chắc chắn vào thời điểm hiện tại", Google TAG nói với The Hacker News khi được hỏi liệu Exotic Lily có thể là một phần mở rộng khác hay không của nhóm Nhện phù thủy. "Trong các rò rỉ của Conti, các thành viên Conti đề cập đến 'những người gửi thư rác' như một người mà họ làm việc cùng (ví dụ: cung cấp các mẫu phần mềm độc hại 'được mã hóa' tùy chỉnh, v.v.) thông qua việc thuê ngoài. Tuy nhiên, hầu hết 'những người gửi thư rác' dường như không có mặt (hoặc tích cực giao tiếp) trong cuộc trò chuyện, do đó dẫn đến kết luận rằng họ đang hoạt động như một thực thể riêng biệt. "  Các chiêu dụ kỹ thuật xã hội của kẻ đe dọa, được gửi từ các tài khoản email giả mạo, đã đặc biệt chỉ ra các lĩnh vực CNTT, an ninh mạng và chăm sóc sức khỏe, mặc dù sau tháng 11 năm 2021, các cuộc tấn công đã trở nên bừa bãi hơn, nhắm vào nhiều tổ chức và ngành công nghiệp khác nhau. Bên cạnh việc sử dụng các công ty hư cấu và danh tính như một phương tiện để xây dựng lòng tin với các thực thể được nhắm mục tiêu, Exotic Lily đã tận dụng các dịch vụ chia sẻ tệp hợp pháp như WeTransfer, TransferNow và OneDrive để phân phối tải trọng BazarBackdoor nhằm trốn tránh các cơ chế phát hiện.  Những kẻ giả mạo thường đóng giả là nhân viên của các công ty như Amazon, hoàn chỉnh với các hồ sơ lừa đảo trên mạng xã hội trên LinkedIn có các ảnh hồ sơ giả do AI tạo. Nhóm này cũng được cho là đã mạo danh nhân viên thực của công ty bằng cách xóa dữ liệu cá nhân của họ khỏi các phương tiện truyền thông xã hội và cơ sở dữ liệu kinh doanh như RocketReach và CrunchBase.  "Ở giai đoạn cuối cùng, kẻ tấn công sẽ tải trọng tải lên dịch vụ chia sẻ tệp công khai (TransferNow, TransferXL, WeTransfer hoặc OneDrive) và sau đó sử dụng tính năng thông báo email tích hợp để chia sẻ tệp với mục tiêu, cho phép gửi email cuối cùng. bắt nguồn từ địa chỉ email của một dịch vụ chia sẻ tệp hợp pháp chứ không phải email của kẻ tấn công, điều này gây ra những thách thức phát hiện bổ sung ", các nhà nghiên cứu cho biết. Cũng được phân phối bằng cách sử dụng khai thác MHTML là một trình tải tùy chỉnh có tên Bumblebee được điều khiển để thu thập và lấy thông tin hệ thống đến một máy chủ từ xa, máy chủ này sẽ phản hồi lại các lệnh để thực thi shellcode và chạy các tệp thực thi ở giai đoạn tiếp theo, bao gồm cả Cobalt Strike. Một phân tích về hoạt động giao tiếp của Exotic Lily chỉ ra rằng những kẻ đe dọa có "công việc điển hình từ 9 đến 5" vào các ngày trong tuần và có thể đang làm việc từ múi giờ Trung hoặc Đông Âu. "Exotic Lily dường như hoạt động như một thực thể riêng biệt, tập trung vào việc có được quyền truy cập ban đầu thông qua các chiến dịch email, với các hoạt động tiếp theo bao gồm triển khai Conti và Diavol ransomware, được thực hiện bởi một nhóm tác nhân khác nhau", các nhà nghiên cứu kết luận.   Tìm thấy bài viết này thú vị? Theo dõi THN trên Facebook, Twitter  và LinkedIn để đọc thêm nội dung độc quyền mà chúng tôi đăng. |

# New Variant of Russian Cyclops Blink Botnet Targeting ASUS Routers

📅Date: March 17, 2022 👤Author: Ravie Lakshmanan

Link tham khảo: *https://thehackernews.com/2022/03/new-variant-of-russian-cyclops-blink.html*



|  |  |
| --- | --- |
| Title: 🐄New Variant of Russian Cyclops Blink Botnet Targeting ASUS Routers | Title: 🐄Biến thể mới của Botnet Cyclops Blink của Nga Nhắm mục tiêu các Bộ định tuyến ASUS |
| ASUS routers have emerged as the target of a nascent botnet called Cyclops Blink, almost a month after it was revealed the malware abused WatchGuard firewall appliances as a stepping stone to gain remote access to breached networks. According to a new report published by Trend Micro, the botnet's "main purpose is to build an infrastructure for further attacks on high-value targets," given that none of the infected hosts "belong to critical organizations, or those that have an evident value on economic, political, or military espionage." Intelligence agencies from the U.K. and the U.S. have characterized Cyclops Blink as a replacement framework for VPNFilter, another malware that has exploited network devices, primarily small office/home office (SOHO) routers, and network-attached storage (NAS) devices.  Both VPNFilter and Cyclops Blink have been attributed to a Russian state-sponsored actor tracked as Sandworm (aka Voodoo Bear), which has also been linked to a number of high-profile intrusions, including that of the 2015 and 2016 attacks on the Ukrainian electrical grid, the 2017 NotPetya attack, and the 2018 Olympic Destroyer attack on the Winter Olympic Games. Written in the C language, the advanced modular botnet affects a number of ASUS router models, with the company acknowledging that it's working on an update to address any potential exploitation –  GT-AC5300 firmware under 3.0.0.4.386.xxxx GT-AC2900 firmware under 3.0.0.4.386.xxxx RT-AC5300 firmware under 3.0.0.4.386.xxxx RT-AC88U firmware under 3.0.0.4.386.xxxx RT-AC3100 firmware under 3.0.0.4.386.xxxx RT-AC86U firmware under 3.0.0.4.386.xxxx RT-AC68U, AC68R, AC68W, AC68P firmware under 3.0.0.4.386.xxxx RT-AC66U\_B1 firmware under 3.0.0.4.386.xxxx RT-AC3200 firmware under 3.0.0.4.386.xxxx RT-AC2900 firmware under 3.0.0.4.386.xxxx RT-AC1900P, RT-AC1900P firmware under 3.0.0.4.386.xxxx RT-AC87U (end-of-life) RT-AC66U (end-of-life), and RT-AC56U (end-of-life)  Cyclops Blink, besides using OpenSSL to encrypt communications with its command-and-control (C2) servers, also incorporates specialized modules that can read and write from the devices' flash memory, granting it the ability to achieve persistence and survive factory resets. A second reconnaissance module serves as a channel for exfiltrating information from the hacked device back to the C2 server, while a file download component takes charge of retrieving arbitrary payloads optionally via HTTPS.  The exact mode of initial access is currently not known, but Cyclops Blink is said to have impacted WatchGuard devices and Asus routers located in the U.S., India, Italy, Canada, and Russia since June 2019. Some of the affected hosts belong to a law firm in Europe, a medium-sized entity producing medical equipment for dentists in Southern Europe, and a plumbing company in the U.S. With IoT devices and routers becoming a lucrative attack surface due to the infrequency of patching and the absence of security software, Trend Micro warned that this could lead to the formation of "eternal botnets." "Once an IoT device is infected with malware, an attacker can have unrestricted internet access for downloading and deploying more stages of malware for reconnaissance, espionage, proxying, or anything else that the attacker wants to do," the researchers said. "In the case of Cyclops Blink, we have seen devices that were compromised for over 30 months (about two and a half years) in a row and were being set up as stable command-and-control servers for other bots."   Found this article interesting? Follow THN on Facebook, Twitter  and LinkedIn to read more exclusive content we post. | Các bộ định tuyến của ASUS đã trở thành mục tiêu của một mạng botnet mới ra đời có tên là Cyclops Blink, gần một tháng sau khi nó được tiết lộ rằng phần mềm độc hại đã lạm dụng các thiết bị tường lửa WatchGuard như một bước đệm để truy cập từ xa vào các mạng bị xâm phạm. Theo một báo cáo mới được công bố bởi Trend Micro, "mục đích chính của mạng botnet là xây dựng cơ sở hạ tầng cho các cuộc tấn công tiếp theo vào các mục tiêu có giá trị cao", với điều kiện không có máy chủ nào bị nhiễm "thuộc các tổ chức quan trọng hoặc những tổ chức có giá trị rõ ràng về kinh tế, chính trị hoặc gián điệp quân sự. " Các cơ quan tình báo của Vương quốc Anh và Hoa Kỳ đã mô tả Cyclops Blink là một khuôn khổ thay thế cho VPNFilter, một phần mềm độc hại khác đã khai thác các thiết bị mạng, chủ yếu là các bộ định tuyến văn phòng / văn phòng nhỏ (SOHO) và các thiết bị lưu trữ gắn mạng (NAS).  Cả VPNFilter và Cyclops Blink đều được cho là do một diễn viên do nhà nước Nga tài trợ, được theo dõi là Sandworm (hay còn gọi là Gấu Voodoo), cũng có liên quan đến một số vụ xâm nhập nổi tiếng, bao gồm cả vụ tấn công năm 2015 và 2016 nhằm vào điện lực Ukraine. lưới điện, cuộc tấn công NotPetya năm 2017 và cuộc tấn công của Kẻ hủy diệt Olympic 2018 vào Thế vận hội Olympic mùa đông. Được viết bằng ngôn ngữ C, mạng botnet mô-đun tiên tiến ảnh hưởng đến một số mẫu bộ định tuyến ASUS, công ty thừa nhận rằng họ đang tiến hành cập nhật để giải quyết mọi khả năng bị khai thác -  Phần sụn GT-AC5300 dưới 3.0.0.4.386.xxxx Phần sụn GT-AC2900 dưới 3.0.0.4.386.xxxx Phần mềm RT-AC5300 dưới 3.0.0.4.386.xxxx Phần mềm RT-AC88U dưới 3.0.0.4.386.xxxx Phần mềm RT-AC3100 dưới 3.0.0.4.386.xxxx Phần mềm RT-AC86U dưới 3.0.0.4.386.xxxx RT-AC68U, AC68R, AC68W, AC68P firmware theo 3.0.0.4.386.xxxx RT-AC66U\_B1 firmware dưới 3.0.0.4.386.xxxx Phần mềm RT-AC3200 dưới 3.0.0.4.386.xxxx Phần mềm RT-AC2900 dưới 3.0.0.4.386.xxxx RT-AC1900P, RT-AC1900P firmware dưới 3.0.0.4.386.xxxx RT-AC87U (hết tuổi thọ) RT-AC66U (hết tuổi thọ) và RT-AC56U (hết tuổi thọ)  Cyclops Blink, bên cạnh việc sử dụng OpenSSL để mã hóa thông tin liên lạc với các máy chủ điều khiển và kiểm soát (C2), còn kết hợp các mô-đun chuyên dụng có thể đọc và ghi từ bộ nhớ flash của thiết bị, cho phép nó hoạt động bền bỉ và tồn tại khi đặt lại tại nhà máy. Mô-đun trinh sát thứ hai đóng vai trò như một kênh để lấy thông tin từ thiết bị bị tấn công trở lại máy chủ C2, trong khi một thành phần tải xuống tệp chịu trách nhiệm truy xuất các tải trọng tùy ý theo tùy chọn thông qua HTTPS.  Phương thức truy cập ban đầu chính xác hiện chưa được xác định, nhưng Cyclops Blink được cho là đã ảnh hưởng đến các thiết bị WatchGuard và bộ định tuyến của Asus đặt tại Hoa Kỳ, Ấn Độ, Ý, Canada và Nga kể từ tháng 6 năm 2019. Một số máy chủ bị ảnh hưởng phải tuân theo luật công ty ở Châu Âu, một công ty quy mô vừa sản xuất thiết bị y tế cho nha sĩ ở Nam Âu, và một công ty hệ thống ống nước ở Mỹ Với việc các thiết bị IoT và bộ định tuyến đang trở thành một bề mặt tấn công béo bở do không thường xuyên vá lỗi và không có phần mềm bảo mật, Trend Micro cảnh báo rằng điều này có thể dẫn đến sự hình thành của "các mạng botnet vĩnh cửu". Các nhà nghiên cứu cho biết: "Một khi thiết bị IoT bị nhiễm phần mềm độc hại, kẻ tấn công có thể có quyền truy cập internet không giới hạn để tải xuống và triển khai nhiều giai đoạn phần mềm độc hại hơn để do thám, gián điệp, ủy quyền hoặc bất cứ điều gì khác mà kẻ tấn công muốn thực hiện". "Trong trường hợp của Cyclops Blink, chúng tôi đã thấy các thiết bị bị xâm phạm trong hơn 30 tháng (khoảng hai năm rưỡi) liên tiếp và đang được thiết lập làm máy chủ điều khiển và ra lệnh ổn định cho các bot khác."   Tìm thấy bài viết này thú vị? Theo dõi THN trên Facebook, Twitter  và LinkedIn để đọc thêm nội dung độc quyền mà chúng tôi đăng. |

# Popular NPM Package Updated to Wipe Russia, Belarus Systems to Protest Ukraine Invasion

📅Date: March 17, 2022 👤Author: Ravie Lakshmanan

Link tham khảo: *https://thehackernews.com/2022/03/popular-npm-package-updated-to-wipe.html*

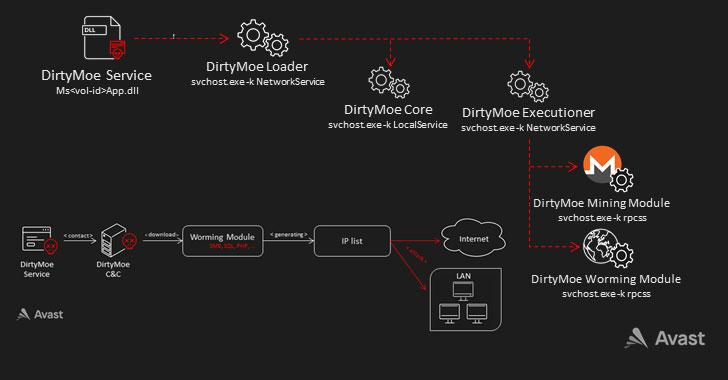


|  |  |
| --- | --- |
| Title: 🐄Popular NPM Package Updated to Wipe Russia, Belarus Systems to Protest Ukraine Invasion | Title: 🐄Gói NPM phổ biến được cập nhật để xóa sổ các hệ thống Nga, Belarus để phản đối Ukraine xâm lược |
| In what's an act of deliberate sabotage, the developer behind the popular "node-ipc" NPM package shipped a new tampered version to condemn Russia's invasion of Ukraine, raising concerns about security in the open-source and the software supply chain. Affecting versions 10.1.1 and 10.1.2 of the library, the alterations introduced by its maintainer RIAEvangelist brought about undesirable behavior by targeting users with IP addresses located either in Russia or Belarus, and wiping arbitrary file contents and replacing them with a heart emoji. Node-ipc is a prominent node module used for local and remote inter-process communication (IPC) with support for Linux, macOS, and Windows. It has over 1.1 million weekly downloads.  "A very clear abuse and a critical supply chain security incident will occur for any system on which this NPM package will be called upon, if that matches a geo-location of either Russia or Belarus," Synk researcher Liran Tal said in an analysis. The issue has been assigned the identifier CVE-2022-23812 and is rated 9.8 out of 10 on the CVSS vulnerability scoring system. The malicious code changes were published on March 7 (version 10.1.1), with a second update occurring 10 hours later the same day (version 10.1.1). Interestingly, although the destructive modifications were removed from the library with version 10.1., a major update was pushed after less than four hours (version 11.0.0), which imported another dependency called "peacenotwar," also released by RIAEvangelist as a form of "non-violent protest against Russia's aggression."  "Any time the node-ipc module functionality gets called, it prints to STDOUT a message taken out of the peacenotwar module, as well as places a file on the user's Desktop directory with contents relating to the current war-time situation of Russia and Ukraine," Tal explained. As of March 15, 2022, the latest version of node-ipc – 11.1.0 – bumps the "peacenotwar" package version from 9.1.3 to 9.1.5 and bundles the "colors" NPM library, while also removing the STDOUT console messages. It's worth noting that "colors," along with another package called "faker," were both intentionally sabotaged earlier this January by its developer Marak Squires by introducing infinite loops to the source code, effectively breaking other applications that depended on the libraries.  According to Bleeping Computer, which first reported the corruption, the changes are said to have been retaliatory, with the developer noting that "Respectfully, I am no longer going to support Fortune 500s (and other smaller sized companies) with my free work." If anything, the idea of using popular modules as "protestware" to deploy destructive payloads and stage a supply chain compromise runs the risk of undermining trust in open-source software. "This security incident involves destructive acts of corrupting files on disk by one maintainer and their attempts to hide and restate that deliberate sabotage in different forms," Tal said. "While this is an attack with protest-driven motivations, it highlights a larger issue facing the software supply chain: the transitive dependencies in your code can have a huge impact on your security."   Found this article interesting? Follow THN on Facebook, Twitter  and LinkedIn to read more exclusive content we post. | Trong một hành động cố ý phá hoại, nhà phát triển đằng sau gói NPM "node-ipc" phổ biến đã vận chuyển một phiên bản giả mạo mới để lên án cuộc xâm lược của Nga vào Ukraine, làm dấy lên lo ngại về an ninh trong chuỗi cung ứng phần mềm và mã nguồn mở. Ảnh hưởng đến các phiên bản 10.1.1 và 10.1.2 của thư viện, những thay đổi do người bảo trì RIAEvangelist đưa ra đã dẫn đến hành vi không mong muốn bằng cách nhắm mục tiêu người dùng có địa chỉ IP ở Nga hoặc Belarus, đồng thời xóa nội dung tệp tùy ý và thay thế chúng bằng biểu tượng cảm xúc trái tim. Node-ipc là một mô-đun nút nổi bật được sử dụng để giao tiếp giữa các quá trình cục bộ và từ xa (IPC) với sự hỗ trợ cho Linux, macOS và Windows. Nó có hơn 1,1 triệu lượt tải xuống hàng tuần.  Nhà nghiên cứu Liran Tal của Synk cho biết: “Một sự lạm dụng rất rõ ràng và một sự cố an ninh chuỗi cung ứng nghiêm trọng sẽ xảy ra đối với bất kỳ hệ thống nào mà gói NPM này sẽ được sử dụng, nếu nó khớp với vị trí địa lý của Nga hoặc Belarus,” nhà nghiên cứu Liran Tal của Synk cho biết. Sự cố đã được gán mã nhận dạng CVE-2022-23812 và được xếp hạng 9,8 trên 10 trên hệ thống chấm điểm lỗ hổng CVSS. Các thay đổi về mã độc được công bố vào ngày 7 tháng 3 (phiên bản 10.1.1), với bản cập nhật thứ hai xảy ra vào 10 giờ sau cùng ngày (phiên bản 10.1.1). Điều thú vị là, mặc dù các sửa đổi phá hoại đã bị xóa khỏi thư viện với phiên bản 10.1., Một bản cập nhật lớn đã được đẩy sau chưa đầy bốn giờ (phiên bản 11.0.0), đã nhập một phần phụ thuộc khác có tên là "hòa bình", cũng được phát hành bởi RIAEvangelist dưới dạng "phản đối bất bạo động chống lại sự xâm lược của Nga."  "Bất cứ khi nào chức năng mô-đun node-ipc được gọi, nó sẽ in tới STDOUT một thông báo được đưa ra khỏi mô-đun hòa bình, cũng như đặt một tệp trên thư mục Desktop của người dùng có nội dung liên quan đến tình hình thời chiến hiện tại của Nga và Ukraine , ”Tal giải thích. Kể từ ngày 15 tháng 3 năm 2022, phiên bản mới nhất của node-ipc - 11.1.0 - gặp phiên bản gói "hòa bình" từ 9.1.3 thành 9.1.5 và gói thư viện NPM "màu", đồng thời xóa thông báo bảng điều khiển STDOUT . Cần lưu ý rằng "màu sắc", cùng với một gói khác có tên "faker", đều đã bị nhà phát triển Marak Squires cố ý phá hoại vào đầu tháng Giêng này bằng cách giới thiệu các vòng lặp vô hạn cho mã nguồn, phá vỡ hiệu quả các ứng dụng khác phụ thuộc vào các thư viện.  Theo Bleeping Computer, công ty đầu tiên báo cáo vụ tham nhũng, những thay đổi được cho là để trả đũa, với nhà phát triển lưu ý rằng "Trân trọng, tôi sẽ không còn hỗ trợ Fortune 500 (và các công ty có quy mô nhỏ hơn) với công việc miễn phí của tôi." Nếu bất cứ điều gì, ý tưởng sử dụng các mô-đun phổ biến làm "phần mềm phản kháng" để triển khai các tải trọng phá hoại và tạo ra một thỏa hiệp chuỗi cung ứng có nguy cơ làm xói mòn niềm tin vào phần mềm nguồn mở. "Sự cố bảo mật này liên quan đến các hành vi phá hoại làm hỏng các tệp trên đĩa của một người bảo trì và nỗ lực của họ để che giấu và trình bày lại hành vi phá hoại có chủ ý đó dưới các hình thức khác nhau", Tal nói. "Mặc dù đây là một cuộc tấn công với động cơ phản đối, nhưng nó làm nổi bật một vấn đề lớn hơn mà chuỗi cung ứng phần mềm phải đối mặt: các phụ thuộc mang tính bắc cầu trong mã của bạn có thể có tác động rất lớn đến bảo mật của bạn."   Tìm thấy bài viết này thú vị? Theo dõi THN trên Facebook, Twitter  và LinkedIn để đọc thêm nội dung độc quyền mà chúng tôi đăng. |

# DirtyMoe Botnet Gains New Exploits in Wormable Module to Spread Rapidly

📅Date: March 17, 2022 👤Author: Ravie Lakshmanan

Link tham khảo: *https://thehackernews.com/2022/03/dirtymoe-botnet-gains-new-exploits-in.html*



|  |  |
| --- | --- |
| Title: 🐄DirtyMoe Botnet Gains New Exploits in Wormable Module to Spread Rapidly | Title: 🐄Botnet DirtyMoe thu được các khai thác mới trong mô-đun Wormable để lan truyền nhanh chóng |
| The malware known as DirtyMoe has gained new worm-like propagation capabilities that allow it to expand its reach without requiring any user interaction, the latest research has found. "The worming module targets older well-known vulnerabilities, e.g., EternalBlue and Hot Potato Windows privilege escalation," Avast researcher Martin Chlumecký said in a report published Wednesday. "One worm module can generate and attack hundreds of thousands of private and public IP addresses per day; many victims are at risk since many machines still use unpatched systems or weak passwords."  Active since 2016, the DirtyMoe botnet is used for carrying out cryptojacking and distributed denial-of-service (DDoS) attacks, and is deployed by means of external exploit kits like PurpleFox or injected installers of Telegram Messenger. Also employed as part of the attack sequence is a DirtyMoe service that triggers the launch of two additional processes, namely the Core and the Executioner, which is used to load the modules for Monero mining and to spread the malware in a worm-like manner.  The worming modules attack victim machines by using several vulnerabilities to install the malware, with each module targeting a specific flaw based on information gathered post reconnaissance –  CVE-2019-9082: ThinkPHP – Multiple PHP Injection RCEs CVE-2019-2725: Oracle Weblogic Server – 'AsyncResponseService' Deserialization RCE CVE-2019-1458: WizardOpium Local Privilege Escalation CVE-2018-0147: Deserialization Vulnerability CVE-2017-0144: EternalBlue SMB Remote Code Execution (MS17-010) MS15-076: RCE Allow Elevation of Privilege (Hot Potato Windows Privilege Escalation) Dictionary attacks aimed at MS SQL Servers, SMB, and Windows Management Instrumentation (WMI) services with weak passwords   "The main goal of the worming module is to achieve RCE under administrator privileges and install a new DirtyMoe instance," Chlumecký explained, adding one of the component's core functions is to generate a list of IP addresses to attack based on the geological location of the module. Furthermore, another in-development worming module was found to contain exploits targeting PHP, Java Deserialization, and Oracle Weblogic Servers, implying that the attackers are looking to broaden the scope of the infections. "Worming target IPs are generated utilizing the cleverly designed algorithm that evenly generates IP addresses across the world and in relation to the geological location of the worming module," Chlumecký said. "Moreover, the module targets local/home networks. Because of this, public IPs and even private networks behind firewalls are at risk."   Found this article interesting? Follow THN on Facebook, Twitter  and LinkedIn to read more exclusive content we post. | Theo nghiên cứu mới nhất, phần mềm độc hại được gọi là DirtyMoe đã có được khả năng lây lan giống như sâu mới cho phép nó mở rộng phạm vi tiếp cận mà không cần bất kỳ sự tương tác nào của người dùng, nghiên cứu mới nhất đã phát hiện ra. Nhà nghiên cứu Martin Chlumecký của Avast cho biết trong một báo cáo được công bố hôm thứ Tư: "Mô-đun tẩy giun nhắm mục tiêu vào các lỗ hổng nổi tiếng cũ hơn, ví dụ: EternalBlue và Hot Potato nâng cấp đặc quyền Windows". "Một mô-đun sâu có thể tạo và tấn công hàng trăm nghìn địa chỉ IP riêng và công khai mỗi ngày; nhiều nạn nhân đang gặp rủi ro vì nhiều máy vẫn sử dụng hệ thống chưa được vá hoặc mật khẩu yếu."  Hoạt động từ năm 2016, mạng botnet DirtyMoe được sử dụng để thực hiện các cuộc tấn công từ chối dịch vụ (DDoS) bằng tiền điện tử và phân tán, đồng thời được triển khai bằng các bộ công cụ khai thác bên ngoài như PurpleFox hoặc các trình cài đặt được chèn vào Telegram Messenger. Cũng được sử dụng như một phần của chuỗi tấn công là dịch vụ DirtyMoe kích hoạt khởi chạy hai quy trình bổ sung, đó là Core và Executioner, được sử dụng để tải các mô-đun cho khai thác Monero và phát tán phần mềm độc hại theo cách giống như sâu.  Các mô-đun tẩy giun tấn công máy nạn nhân bằng cách sử dụng một số lỗ hổng để cài đặt phần mềm độc hại, với mỗi mô-đun nhắm vào một lỗ hổng cụ thể dựa trên thông tin thu thập được sau khi do thám -  CVE-2019-9082: ThinkPHP - Nhiều RCE tiêm PHP CVE-2019-2725: Oracle Weblogic Server - 'AsyncResponseService' Deserialization RCE CVE-2019-1458: Nâng cấp đặc quyền địa phương WizardOpium CVE-2018-0147: Lỗ hổng giải mã hóa CVE-2017-0144: Thực thi mã từ xa EternalBlue SMB (MS17-010) MS15-076: RCE Cho phép Nâng cấp Đặc quyền (Nâng cấp Đặc quyền Hot Potato Windows) Các cuộc tấn công từ điển nhằm vào Máy chủ MS SQL, SMB và các dịch vụ Công cụ quản lý Windows (WMI) với mật khẩu yếu   "Mục tiêu chính của mô-đun tẩy giun là đạt được RCE dưới đặc quyền của quản trị viên và cài đặt phiên bản DirtyMoe mới", Chlumecký giải thích, thêm một trong những chức năng cốt lõi của thành phần là tạo danh sách địa chỉ IP để tấn công dựa trên vị trí địa chất của mô-đun. Hơn nữa, một mô-đun tẩy giun khác đang trong quá trình phát triển được phát hiện có chứa các hành vi khai thác nhắm mục tiêu vào Máy chủ PHP, Java Deserialization và Oracle Weblogic Server, ngụ ý rằng những kẻ tấn công đang muốn mở rộng phạm vi lây nhiễm. Chlumecký cho biết: “Các IP mục tiêu diệt mối được tạo ra bằng cách sử dụng thuật toán được thiết kế thông minh để tạo ra các địa chỉ IP đồng đều trên toàn thế giới và liên quan đến vị trí địa chất của mô-đun tẩy giun”. "Hơn nữa, mô-đun nhắm mục tiêu các mạng cục bộ / gia đình. Do đó, các IP công cộng và thậm chí cả các mạng riêng nằm sau tường lửa đều có nguy cơ."   Tìm thấy bài viết này thú vị? Theo dõi THN trên Facebook, Twitter  và LinkedIn để đọc thêm nội dung độc quyền mà chúng tôi đăng. |

# The Golden Hour of Incident Response

📅Date: March 17, 2022 👤Author: The Hacker News

Link tham khảo: *https://thehackernews.com/2022/03/the-golden-hour-of-incident-response.html*

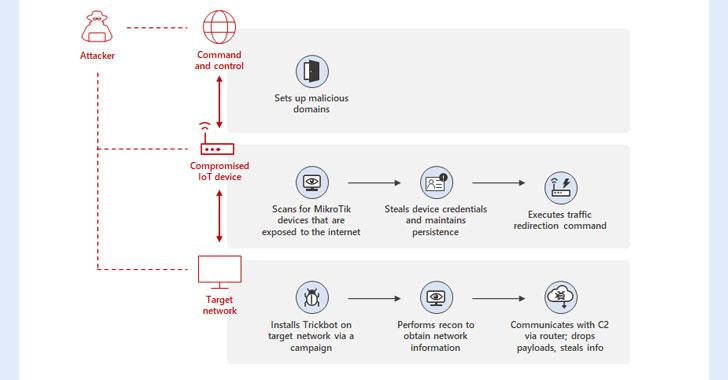


|  |  |
| --- | --- |
| Title: 🐄The Golden Hour of Incident Response | Title: 🐄Giờ vàng ứng phó sự cố |
| As a CSIRT consultant, I cannot overemphasize the importance of effectively managing the first hour in a critical incident. Finding out what to do is often a daunting task in a critical incident. In addition, the feeling of uneasiness often prevents an incident response analyst from making effective decisions. However, keeping a cool head and actions planned out is crucial in successfully handling a security incident. This blog will elaborate on some key points to help readers facilitate better incident response procedures.  Preparation is essential Before taking on any incidents, security analysts would need to know a great deal of information. To start off, incident response analysts need to familiarize themselves with their roles and responsibilities. IT infrastructure has evolved rapidly over the past years. For example, we observed increasing movement to cloud computing and data storage. The fast-changing IT environment frequently requires analysts to update their skill sets, such as learning about cloud security. Consequently, analysts will need to have hands-on practice and maintain a complete picture of the topology of all systems. In the real world, external CSIRT analysts should quickly identify all assets under their responsibility. At the same time, the in-house CSIRT analysts should also actively participate in the vulnerability management and the discovery scanning processes.  The quality of collected information determines the outcomes of incident response. In addition, the CSIRT analysts would also need to understand the threats they will be facing. As defensive cyber security technologies are upgraded each day, the threat actors are poised to evolve. For example, according to a paper in 2020, four out of the top ten active ransomware actors are now using the "Ransomware as a service" business model [1]. This pattern denotes that malicious actors will more easily deploy ransomware because of the lack of technical requirements to leverage such attacks. After all, CSIRT teams need to identify the primary threats they are likely to encounter. For example, a CSIRT specialist may see common malware and conclude that no additional threats exist. But when this situation arises for more sensitive scenarios, such as an attack in the energy sector, they will have to think critically and look out for unconventional attack methods. To effectively prepare for incident response, the analysts need to be familiar with the infrastructure they will be working with and the cyber security threat landscape they will be facing.  Get robust procedures in place Knowing is only half the battle. When the alert sounds, we need to calm ourselves quickly and plan to answer the first question, "what should I do in the first hour?" The paper "Phases of a Critical Incident" refers to the first hour in a critical incident as the "crisis phase" and is "characterized by confusion, panic, rush to the scene, and gridlock."[2] Well-rehearsed CSIRT analysts do well to exercise discernment in their investigation.  On the other hand, in many scenarios, they may be prone to the obscurity of information, the inability to effectuate a solution in a limited time frame, and lack of operational jurisdiction. In such times, the incident response team must take matters into their own hands, clearly express their professional knowledge, and push through with their operations.  When performing the investigation and root-cause analysis, the incident response team often gets stuck on finding missing pieces of the puzzle. These difficulties lead to doubt and indecision.  In such events, the analysts often speculate the incident to be caused by one or more possibilities of a breach without certainty. In these circumstances, it's advised for them to assume the most likely cause and act accordingly. In the first hour, time is imperative. Like taking an exam, where time is limited, skip the questions you're stuck on first.  Nowadays, the incident response containment process is often simplified due to the widely adopted Endpoint Detection and Response (EDR) technologies, which offer network containment capabilities at the push of a button. Nonetheless, even with traditional network containment tools, containing the network is not always an easy one. People do not always choose the safer option when it is available. But as the saying goes, it's always better to be safe than sorry!  Find out what really happened and close the gaps Perhaps after one hour, there are still pieces of the puzzle left missing. Now it's a good idea to take some time and reflect upon all the possibilities and work down a list.  For example, I handled a security incident where the attacker launched a reverse shell on a server. I immediately decided to contain the server and gathered all evidence. But my teammates and I still couldn't figure out how the server was compromised, so we made a list of all the accessible services and examined relevant logs for each service.  Initial speculations put an IT operation tool as the indicator of compromise. But eventually, we overrode this speculation by crossing out all possibilities and concluded that there must be an inherent security flaw in its web service.  From time to time, during the post-breach analysis, CSIRT analysts may encounter setbacks in connecting the dots. But the truth will always prevail with enough patience and a correct mindset. What you should consider In conclusion, effectively managing the crucial one-hour time interval after a critical incident requires more than learning on the spot.  In addition to technical specialties, experienced CSIRT analysts will also benefit from extensive preparation on their assets and their adversaries, prioritization of tasks and making quick decisions when required, as well as being able to discern down-to-earth facts using the process of elimination. This is just another excerpt of the stories in the Security Navigator. Other interesting stuff like actual CSIRT- and pentesting operations, as well as tons of facts and figures on the security landscape in general can be found there as well. The full report is available for download on the Orange Cyberdefense website, so have a look. It's worth it! [1] Midler, Marisa. "Ransomware as a Service (Raas) Threats." SEI Blog, 5 Oct. 2020, https://insights.sei.cmu.edu/blog/ransomware-as-a-service-raas-threats/ [2] "Phases of a Critical Incident." Eddusaver, 5 May 2020, https://www.eddusaver.com/phases-of-a-critical-incident/ Note — This article was written and contributed by Tingyang Wei, Security Analyst at Orange Cyberdefense.   Found this article interesting? Follow THN on Facebook, Twitter  and LinkedIn to read more exclusive content we post. | Là một nhà tư vấn CSIRT, tôi không thể nhấn mạnh quá tầm quan trọng của việc quản lý hiệu quả trong giờ đầu tiên trong một sự cố quan trọng. Tìm ra những gì cần làm thường là một nhiệm vụ khó khăn trong một sự cố quan trọng. Ngoài ra, cảm giác không yên tâm thường ngăn cản một nhà phân tích phản ứng sự cố đưa ra các quyết định hiệu quả. Tuy nhiên, giữ một cái đầu lạnh và các hành động được lên kế hoạch là rất quan trọng để xử lý thành công một sự cố an ninh. Blog này sẽ trình bày chi tiết về một số điểm chính để giúp người đọc tạo điều kiện thuận lợi hơn cho các thủ tục ứng phó sự cố.  Chuẩn bị là cần thiết Trước khi xử lý bất kỳ sự cố nào, các nhà phân tích bảo mật sẽ cần biết rất nhiều thông tin. Để bắt đầu, các nhà phân tích ứng phó sự cố cần tự làm quen với vai trò và trách nhiệm của họ. Cơ sở hạ tầng CNTT đã phát triển nhanh chóng trong những năm qua. Ví dụ: chúng tôi đã quan sát thấy sự chuyển động ngày càng tăng đối với điện toán đám mây và lưu trữ dữ liệu. Môi trường CNTT thay đổi nhanh thường xuyên đòi hỏi các nhà phân tích phải cập nhật bộ kỹ năng của họ, chẳng hạn như tìm hiểu về bảo mật đám mây. Do đó, các nhà phân tích sẽ cần phải thực hành thực tế và duy trì một bức tranh toàn cảnh về cấu trúc liên kết của tất cả các hệ thống. Trong thế giới thực, các nhà phân tích CSIRT bên ngoài nên nhanh chóng xác định tất cả các tài sản thuộc trách nhiệm của họ. Đồng thời, các nhà phân tích CSIRT nội bộ cũng nên tham gia tích cực vào việc quản lý lỗ hổng bảo mật và quy trình quét khám phá. Chất lượng của thông tin thu thập xác định kết quả của ứng phó sự cố. Ngoài ra, các nhà phân tích CSIRT cũng cần hiểu những mối đe dọa mà họ sẽ phải đối mặt. Khi các công nghệ an ninh mạng phòng thủ được nâng cấp mỗi ngày, các tác nhân đe dọa đang sẵn sàng phát triển. Ví dụ, theo một bài báo vào năm 2020, bốn trong số mười tác nhân ransomware hoạt động hàng đầu hiện đang sử dụng mô hình kinh doanh "Ransomware như một dịch vụ" [1]. Mô hình này biểu thị rằng các tác nhân độc hại sẽ dễ dàng triển khai ransomware hơn vì thiếu các yêu cầu kỹ thuật để tận dụng các cuộc tấn công như vậy. Sau cùng, các nhóm CSIRT cần xác định các mối đe dọa chính mà họ có thể gặp phải. Ví dụ: một chuyên gia CSIRT có thể thấy phần mềm độc hại phổ biến và kết luận rằng không có mối đe dọa bổ sung nào tồn tại. Nhưng khi tình huống này xảy ra đối với các kịch bản nhạy cảm hơn, chẳng hạn như một cuộc tấn công trong lĩnh vực năng lượng, họ sẽ phải suy nghĩ chín chắn và tìm ra các phương pháp tấn công độc đáo. Để chuẩn bị hiệu quả cho ứng phó sự cố, các nhà phân tích cần phải quen thuộc với cơ sở hạ tầng mà họ sẽ làm việc và bối cảnh mối đe dọa an ninh mạng mà họ sẽ phải đối mặt.  Nhận các quy trình mạnh mẽ tại chỗ Biết chỉ là một nửa của trận chiến. Khi cảnh báo vang lên, chúng ta cần nhanh chóng lấy lại bình tĩnh và lên kế hoạch trả lời câu hỏi đầu tiên, "tôi nên làm gì trong giờ đầu tiên?" Bài báo "Các giai đoạn của một sự cố nghiêm trọng" đề cập đến giờ đầu tiên trong một sự cố nghiêm trọng là "giai đoạn khủng hoảng" và "được đặc trưng bởi sự bối rối, hoảng sợ, vội vã đến hiện trường và bế tắc." [2] Các nhà phân tích CSIRT đã được diễn tập thành thạo. làm tốt để thực hiện sự sáng suốt trong cuộc điều tra của họ. Mặt khác, trong nhiều trường hợp, họ có thể dễ bị mù mờ thông tin, không có khả năng thực hiện một giải pháp trong một khung thời gian giới hạn và thiếu thẩm quyền điều hành. Trong những lúc như vậy, nhóm ứng phó sự cố phải tự mình giải quyết vấn đề, thể hiện rõ ràng kiến ​​thức chuyên môn của mình và thúc đẩy hoạt động của họ. Khi thực hiện điều tra và phân tích nguyên nhân gốc rễ, đội ứng phó sự cố thường gặp khó khăn trong việc tìm kiếm các mảnh ghép còn thiếu. Những khó khăn này dẫn đến nghi ngờ và do dự. Trong những trường hợp như vậy, các nhà phân tích thường suy đoán sự cố là do một hoặc nhiều khả năng vi phạm mà không chắc chắn. Trong những trường hợp này, họ nên cho rằng nguyên nhân có thể xảy ra nhất và hành động phù hợp. Trong giờ đầu tiên, thời gian là bắt buộc. Giống như tham gia một kỳ thi, khi thời gian có hạn, hãy bỏ qua những câu hỏi bạn đang mắc kẹt trước. Ngày nay, quy trình ngăn chặn ứng phó sự cố thường được đơn giản hóa do các công nghệ Phát hiện và Phản hồi Điểm cuối (EDR) được áp dụng rộng rãi, cung cấp khả năng ngăn chặn mạng chỉ bằng một nút nhấn. Tuy nhiên, ngay cả với các công cụ ngăn chặn mạng truyền thống, việc chứa mạng không phải lúc nào cũng dễ dàng. Không phải lúc nào mọi người cũng chọn phương án an toàn hơn khi nó có sẵn. Nhưng như người ta nói, luôn luôn tốt hơn để được an toàn hơn là xin lỗi!  Tìm hiểu điều gì đã thực sự xảy ra và thu hẹp khoảng cách Có lẽ sau một giờ, vẫn còn thiếu các mảnh ghép. Bây giờ, bạn nên dành một chút thời gian và xem xét tất cả các khả năng và lập danh sách. Ví dụ: tôi đã xử lý một sự cố bảo mật trong đó kẻ tấn công khởi chạy một trình bao đảo ngược trên máy chủ. Tôi ngay lập tức quyết định chứa máy chủ và thu thập tất cả bằng chứng. Nhưng đồng đội của tôi và tôi vẫn không thể tìm ra cách máy chủ bị xâm nhập, vì vậy chúng tôi đã lập danh sách tất cả các dịch vụ có thể truy cập và kiểm tra nhật ký liên quan cho từng dịch vụ. Những suy đoán ban đầu đặt một công cụ vận hành CNTT như là dấu hiệu của sự thỏa hiệp. Nhưng cuối cùng, chúng tôi đã loại bỏ suy đoán này bằng cách loại bỏ tất cả các khả năng và kết luận rằng phải có một lỗ hổng bảo mật cố hữu trong dịch vụ web của nó. Đôi khi, trong quá trình phân tích sau vi phạm, các nhà phân tích của CSIRT có thể gặp phải những trở ngại trong việc kết nối các điểm. Nhưng sự thật sẽ luôn thắng nếu bạn có đủ kiên nhẫn và một suy nghĩ đúng đắn. Những gì bạn nên xem xét Tóm lại, quản lý hiệu quả khoảng thời gian quan trọng một giờ sau một sự cố nghiêm trọng đòi hỏi nhiều hơn là học tại chỗ. Ngoài các chuyên môn kỹ thuật, các nhà phân tích CSIRT có kinh nghiệm cũng sẽ được hưởng lợi từ việc chuẩn bị kỹ lưỡng về tài sản và đối thủ của họ, sắp xếp thứ tự ưu tiên các nhiệm vụ và đưa ra quyết định nhanh chóng khi được yêu cầu, cũng như có thể phân biệt thực tế bằng cách sử dụng quy trình loại bỏ . Đây chỉ là một đoạn trích khác của những câu chuyện trong Bộ điều hướng an ninh. Các nội dung thú vị khác như CSIRT- và các hoạt động dồn nén thực tế, cũng như hàng tấn dữ kiện và số liệu về bối cảnh an ninh nói chung cũng có thể được tìm thấy ở đó. Báo cáo đầy đủ có sẵn để tải xuống trên trang web Orange Cyberdefense, vì vậy hãy xem. Nó có giá trị nó! [1] Midler, Marisa. "Ransomware as a Service (Raas) Đe doạ." SEI Blog, ngày 5 tháng 10 năm 2020, https://insights.sei.cmu.edu/blog/ransomware-as-a-service-raas-threats/ [2] "Các giai đoạn của một sự cố nghiêm trọng." Eddusaver, ngày 5 tháng 5 năm 2020, https://www.eddusaver.com/phases-of-a-critical-incident/ Lưu ý - Bài viết này được viết và đóng góp bởi Tingyang Wei, Nhà phân tích bảo mật tại Orange Cyberdefense.   Tìm thấy bài viết này thú vị? Theo dõi THN trên Facebook, Twitter  và LinkedIn để đọc thêm nội dung độc quyền mà chúng tôi đăng. |

# TrickBot Malware Abusing MikroTik Routers as Proxies for Command-and-Control

📅Date: March 17, 2022 👤Author: Ravie Lakshmanan

Link tham khảo: *https://thehackernews.com/2022/03/trickbot-malware-abusing-hacked-iot.html*



|  |  |
| --- | --- |
| Title: 🐄TrickBot Malware Abusing MikroTik Routers as Proxies for Command-and-Control | Title: 🐄Phần mềm độc hại TrickBot lạm dụng bộ định tuyến MikroTik làm proxy để ra lệnh và điều khiển |
| Microsoft on Wednesday detailed a previously undiscovered technique put to use by the TrickBot malware that involves using compromised Internet of Things (IoT) devices as a go-between for establishing communications with the command-and-control (C2) servers. "By using MikroTik routers as proxy servers for its C2 servers and redirecting the traffic through non-standard ports, TrickBot adds another persistence layer that helps malicious IPs evade detection by standard security systems," Microsoft's Defender for IoT Research Team and Threat Intelligence Center (MSTIC) said.  TrickBot, which emerged as a banking trojan in 2016, has evolved into a sophisticated and persistent threat, with its modular architecture enabling it to adapt its tactics to suit different networks, environments, and devices as well as offer access-as-a-service for next-stage payloads like Conti ransomware. The expansion to TrickBot's capabilities comes amid reports of its infrastructure going offline, even as the botnet has continually refined its features to make its attack framework durable, evade reverse engineering, and maintain the stability of its C2 servers.  Specifically, the new method identified by MSTIC involves leveraging hacked IoT devices such as routers from MikroTik to "create a line of communication between the TrickBot-affected device and the C2 server."  This also entails breaking into the routers by using a combination of methods, namely default passwords, brute-force attacks, or exploiting a now-patched flaw in MikroTik RouterOS (CVE-2018-14847), followed by changing the router's password to maintain access. In the next step, the attackers then issue a network address translation (NAT) command that's designed to redirect traffic between ports 449 and 80 in the router, establishing a path for the TrickBot-infected hosts to communicate with the C2 server. While potential connections between TrickBot and compromised MikroTik hosts were hinted before in November 2018, this is the first time the exact modus operandi has been laid bare open. With the malware reaching its limits last month and no new C2 servers registered since December 2021, it remains to be seen how the malware authors intend to take the operation forward. "As security solutions for conventional computing devices continue to evolve and improve, attackers will explore alternative ways to compromise target networks," the researchers said. "Attack attempts against routers and other IoT devices are not new, and being unmanaged, they can easily be the weakest links in the network."   Found this article interesting? Follow THN on Facebook, Twitter  and LinkedIn to read more exclusive content we post. | Hôm thứ Tư, Microsoft đã trình bày chi tiết về một kỹ thuật chưa được phát hiện trước đây được phần mềm độc hại TrickBot sử dụng liên quan đến việc sử dụng các thiết bị Internet of Things (IoT) bị xâm nhập như một phương tiện để thiết lập liên lạc với các máy chủ lệnh và kiểm soát (C2). "Bằng cách sử dụng bộ định tuyến MikroTik làm máy chủ proxy cho các máy chủ C2 của nó và chuyển hướng lưu lượng truy cập qua các cổng không chuẩn, TrickBot bổ sung một lớp bền vững khác giúp các IP độc hại tránh được sự phát hiện của các hệ thống bảo mật tiêu chuẩn" MSTIC) cho biết.  TrickBot, nổi lên như một trojan ngân hàng vào năm 2016, đã phát triển thành một mối đe dọa tinh vi và dai dẳng, với kiến ​​trúc mô-đun cho phép nó điều chỉnh các chiến thuật của mình để phù hợp với các mạng, môi trường và thiết bị khác nhau cũng như cung cấp quyền truy cập như một dịch vụ cho các tải trọng ở giai đoạn tiếp theo như Conti ransomware. Việc mở rộng các khả năng của TrickBot được đưa ra trong bối cảnh các báo cáo về việc cơ sở hạ tầng của nó đang hoạt động ngoại tuyến, ngay cả khi mạng botnet đã liên tục tinh chỉnh các tính năng của nó để làm cho khung tấn công bền bỉ, tránh kỹ thuật đảo ngược và duy trì sự ổn định của các máy chủ C2 của nó.  Cụ thể, phương pháp mới được MSTIC xác định liên quan đến việc tận dụng các thiết bị IoT bị tấn công như bộ định tuyến từ MikroTik để "tạo ra một đường dây liên lạc giữa thiết bị bị ảnh hưởng bởi TrickBot và máy chủ C2."  Điều này cũng dẫn đến việc đột nhập vào các bộ định tuyến bằng cách sử dụng kết hợp các phương pháp, cụ thể là mật khẩu mặc định, tấn công brute-force hoặc khai thác một lỗ hổng hiện đã được vá trong MikroTik RouterOS (CVE-2018-14847), tiếp theo là thay đổi mật khẩu của bộ định tuyến để duy trì quyền truy cập . Trong bước tiếp theo, những kẻ tấn công sau đó đưa ra lệnh dịch địa chỉ mạng (NAT) được thiết kế để chuyển hướng lưu lượng giữa các cổng 449 và 80 trong bộ định tuyến, thiết lập đường dẫn cho các máy chủ bị nhiễm TrickBot giao tiếp với máy chủ C2. Mặc dù các kết nối tiềm năng giữa TrickBot và các máy chủ MikroTik bị xâm phạm đã được gợi ý trước đó vào tháng 11 năm 2018, nhưng đây là lần đầu tiên mô thức operandi chính xác được công khai. Với việc phần mềm độc hại đạt đến giới hạn vào tháng trước và không có máy chủ C2 mới nào được đăng ký kể từ tháng 12 năm 2021, vẫn còn phải xem các tác giả phần mềm độc hại dự định tiến hành hoạt động như thế nào trong tương lai. Các nhà nghiên cứu cho biết: “Khi các giải pháp bảo mật cho các thiết bị điện toán thông thường tiếp tục phát triển và cải tiến, những kẻ tấn công sẽ khám phá các cách thay thế để xâm phạm mạng mục tiêu”. "Các nỗ lực tấn công nhằm vào bộ định tuyến và các thiết bị IoT khác không phải là mới và không được quản lý, chúng có thể dễ dàng trở thành các liên kết yếu nhất trong mạng."   Tìm thấy bài viết này thú vị? Theo dõi THN trên Facebook, Twitter  và LinkedIn để đọc thêm nội dung độc quyền mà chúng tôi đăng. |

# Ukraine Secret Service Arrests Hacker Helping Russian Invaders

📅Date: March 17, 2022 👤Author: Ravie Lakshmanan

Link tham khảo: *https://thehackernews.com/2022/03/ukraine-secret-service-arrests-hacker.html*



|  |  |
| --- | --- |
| Title: 🐄Ukraine Secret Service Arrests Hacker Helping Russian Invaders | Title: 🐄Cơ quan mật vụ Ukraine bắt giữ hacker giúp đỡ những kẻ xâm lược Nga |
| The Security Service of Ukraine (SBU) said it has detained a "hacker" who offered technical assistance to the invading Russian troops by providing mobile communication services inside the Ukrainian territory. The anonymous suspect is said to have broadcasted text messages to Ukrainian officials, including security officers and civil servants, proposing that they surrender and take the side of Russia. The individual has also been accused of routing phone calls from Russia to the mobile phones of Russian troops in Ukraine.  "Up to a thousand calls were made through this hacker in one day. Many of them are from the top leadership of the enemy army," the SBU alleged, adding it confiscated the equipment that was used to pull off the operation. Besides implicating the hacker for helping Russia make anonymous phone calls to its military forces based in Ukraine, the agency said the hacker passed commands and instructions to different groups of "Russian invaders." "He will be held accountable for all the severity of the law. Because on it is the blood of tens or even hundreds of killed Ukrainians," read the translation of the announcement.  News of the detainment comes as a third strain of data-wiping malware dubbed "CaddyWiper" has been observed in attacks against several dozen systems in a limited number of organizations in Ukraine, close on the heels of HermeticWiper and IsaacWiper coinciding with Russia's invasion of Ukraine last month.  In a separate incident, Reuters last week reported of a cyber attack that disrupted broadband satellite internet access in Ukraine on February 24 between 5 a.m. and 9 a.m. EET, right around the time Russia commenced its full-scale invasion of the country. The digital sabotage crippled satellite modems that are part of Viasat's KA-SAT network.   Found this article interesting? Follow THN on Facebook, Twitter  and LinkedIn to read more exclusive content we post. | Cơ quan An ninh Ukraine (SBU) cho biết họ đã bắt giữ một "hacker" đã đề nghị hỗ trợ kỹ thuật cho quân đội Nga xâm lược bằng cách cung cấp các dịch vụ liên lạc di động bên trong lãnh thổ Ukraine. Nghi phạm ẩn danh được cho là đã phát các tin nhắn văn bản tới các quan chức Ukraine, bao gồm cả các nhân viên an ninh và công chức, đề nghị họ đầu hàng và đứng về phía Nga. Cá nhân này cũng bị cáo buộc định tuyến các cuộc điện thoại từ Nga tới điện thoại di động của quân đội Nga ở Ukraine.  "Có tới một nghìn cuộc gọi được thực hiện thông qua hacker này trong một ngày. Nhiều người trong số họ đến từ lãnh đạo cao nhất của quân đội đối phương", SBU cáo buộc, đồng thời tịch thu các thiết bị được sử dụng để thực hiện chiến dịch. Bên cạnh việc ám chỉ hacker vì đã giúp Nga thực hiện các cuộc điện thoại nặc danh tới các lực lượng quân sự của họ đóng tại Ukraine, cơ quan này cho biết hacker đã chuyển các lệnh và hướng dẫn cho các nhóm "kẻ xâm lược Nga" khác nhau. "Anh ta sẽ phải chịu trách nhiệm về mọi mức độ nghiêm trọng của luật pháp. Bởi vì trên đó là máu của hàng chục, thậm chí hàng trăm người Ukraine bị giết", bản dịch của thông báo.  Tin tức về vụ bắt giữ được đưa ra khi dòng phần mềm độc hại xóa dữ liệu thứ ba có tên là "CaddyWiper" đã được quan sát thấy trong các cuộc tấn công nhằm vào hàng chục hệ thống trong một số tổ chức hạn chế ở Ukraine, theo sau HermeticWiper và IsaacWiper trùng hợp với cuộc xâm lược của Nga vào Ukraine tháng trước.  Trong một vụ việc riêng, Reuters tuần trước đã báo cáo về một cuộc tấn công mạng làm gián đoạn truy cập internet vệ tinh băng thông rộng ở Ukraine vào ngày 24 tháng 2 từ 5 giờ sáng đến 9 giờ sáng theo giờ EET, ngay trong thời điểm Nga bắt đầu cuộc xâm lược toàn diện vào đất nước. Sự phá hoại kỹ thuật số đã làm tê liệt các modem vệ tinh nằm trong mạng KA-SAT của Viasat.   Tìm thấy bài viết này thú vị? Theo dõi THN trên Facebook, Twitter  và LinkedIn để đọc thêm nội dung độc quyền mà chúng tôi đăng. |

# New Vulnerability in CRI-O Engine Lets Attackers Escape Kubernetes Containers

📅Date: March 17, 2022 👤Author: Ravie Lakshmanan

Link tham khảo: *https://thehackernews.com/2022/03/new-vulnerability-in-cri-o-engine-lets.html*



|  |  |
| --- | --- |
| Title: 🐄New Vulnerability in CRI-O Engine Lets Attackers Escape Kubernetes Containers | Title: 🐄Lỗ hổng mới trong CRI-O Engine cho phép những kẻ tấn công thoát khỏi các thùng chứa Kubernetes |
| A newly disclosed security vulnerability in the Kubernetes container engine CRI-O called cr8escape could be exploited by an attacker to break out of containers and obtain root access to the host. "Invocation of CVE-2022-0811 can allow an attacker to perform a variety of actions on objectives, including execution of malware, exfiltration of data, and lateral movement across pods," CrowdStrike researchers John Walker and Manoj Ahuje said in an analysis published this week. A lightweight alternative to Docker, CRI-O is a container runtime implementation of the Kubernetes Container Runtime Interface (CRI) that's used to pull container images from registries and launch an Open Container Initiative (OCI)-compatible runtime such as runC to spawn and run container processes.  The vulnerability is rated 8.8 on the CVSS vulnerability scoring system and affects CRI-O versions 1.19 and later. Following responsible disclosure, patches have been released to address the flaw in version 1.23.2 shipped on March 15, 2022. CVE-2022-0811 stems from a code change introduced in version 1.19 to set kernel options for a pod, resulting in a scenario where a bad actor with permissions to deploy a pod on a Kubernetes cluster using the CRI-O runtime can take advantage of the "kernel.core\_pattern" parameter to achieve container escape and arbitrary code execution as root on any node in the cluster. The parameter "kernel.core\_pattern" is used to specify a pattern name for a core dump, which is a file containing the memory snapshot of a program at a specific time that's typically activated in response to unexpected crashes or when the process terminates abnormally.  "If the first character of the pattern is a '|' [a pipe], the kernel will treat the rest of the pattern as a command to run. The core dump will be written to the standard input of that program instead of to a file," reads the Linux kernel documentation. Therefore, by setting this option to point to a malicious shell script and triggering a core dump, the vulnerability leads to the invocation of the script, effectively achieving remote code execution and granting the adversary the ability to take over the node. "Kubernetes is not necessary to invoke CVE-2022-8011," the researchers pointed out. "An attacker on a machine with CRI-O installed can use it to set kernel parameters all by itself."   Found this article interesting? Follow THN on Facebook, Twitter  and LinkedIn to read more exclusive content we post. | Một lỗ hổng bảo mật mới được tiết lộ trong công cụ chứa Kubernetes CRI-O được gọi là cr8escape có thể bị kẻ tấn công khai thác để thoát ra khỏi vùng chứa và lấy quyền truy cập root vào máy chủ. "Việc mời CVE-2022-0811 có thể cho phép kẻ tấn công thực hiện nhiều hành động khác nhau đối với các mục tiêu, bao gồm thực thi phần mềm độc hại, lấy cắp dữ liệu và chuyển động ngang qua các nhóm", các nhà nghiên cứu của CrowdStrike John Walker và Manoj Ahuje cho biết trong một phân tích được công bố. tuần. Một giải pháp thay thế nhẹ cho Docker, CRI-O là một triển khai thời gian chạy vùng chứa của Giao diện thời gian chạy vùng chứa Kubernetes (CRI) được sử dụng để kéo hình ảnh vùng chứa từ các đăng ký và khởi chạy thời gian chạy tương thích với Sáng kiến ​​vùng chứa mở (OCI) chẳng hạn như runC để sinh sản và chạy các quy trình container.  Lỗ hổng được đánh giá 8,8 trên hệ thống chấm điểm lỗ hổng CVSS và ảnh hưởng đến CRI-O phiên bản 1.19 trở lên. Theo tiết lộ có trách nhiệm, các bản vá lỗi đã được phát hành để giải quyết lỗ hổng trong phiên bản 1.23.2 được xuất xưởng vào ngày 15 tháng 3 năm 2022. CVE-2022-0811 bắt nguồn từ một sự thay đổi mã được giới thiệu trong phiên bản 1.19 để đặt các tùy chọn hạt nhân cho một nhóm, dẫn đến tình huống trong đó một tác nhân xấu có quyền triển khai một nhóm trên một cụm Kubernetes sử dụng thời gian chạy CRI-O có thể lợi dụng tham số "kernel.core\_pattern" để đạt được thoát vùng chứa và thực thi mã tùy ý với tư cách gốc trên bất kỳ nút nào trong cụm. Tham số "kernel.core\_pattern" được sử dụng để chỉ định tên mẫu cho kết xuất lõi, là tệp chứa ảnh chụp nhanh bộ nhớ của một chương trình tại một thời điểm cụ thể thường được kích hoạt để phản ứng với sự cố không mong muốn hoặc khi quá trình kết thúc bất thường.  "Nếu ký tự đầu tiên của mẫu là '|' [a pipe], hạt nhân sẽ coi phần còn lại của mẫu như một lệnh để chạy. Kết xuất lõi sẽ được ghi vào đầu vào chuẩn của chương trình đó thay vì vào một tệp ", đọc tài liệu về nhân Linux. Do đó, bằng cách đặt tùy chọn này để trỏ đến một tập lệnh shell độc hại và kích hoạt một kết xuất lõi, lỗ hổng dẫn đến việc gọi tập lệnh, đạt được hiệu quả thực thi mã từ xa và cấp cho kẻ thù khả năng chiếm lấy nút. "Kubernetes không cần thiết phải gọi CVE-2022-8011", các nhà nghiên cứu chỉ ra. "Kẻ tấn công trên một máy được cài đặt CRI-O có thể sử dụng nó để tự thiết lập các tham số hạt nhân."   Tìm thấy bài viết này thú vị? Theo dõi THN trên Facebook, Twitter  và LinkedIn để đọc thêm nội dung độc quyền mà chúng tôi đăng. |

# New "B1txor20" Linux Botnet Uses DNS Tunnel and Exploits Log4J Flaw

📅Date: March 16, 2022 👤Author: Ravie Lakshmanan

Link tham khảo: *https://thehackernews.com/2022/03/new-b1txor20-linux-botnet-uses-dns.html*



|  |  |
| --- | --- |
| Title: 🐄New "B1txor20" Linux Botnet Uses DNS Tunnel and Exploits Log4J Flaw | Title: 🐄Botnet Linux "B1txor20" mới Sử dụng Đường hầm DNS và Khai thác Lỗ hổng Log4J |
| A previously undocumented backdoor has been observed targeting Linux systems with the goal of corralling the machines into a botnet and acting as a conduit for downloading and installing rootkits. Qihoo 360's Netlab security team called it B1txor20 "based on its propagation using the file name 'b1t,' the XOR encryption algorithm, and the RC4 algorithm key length of 20 bytes."  First observed propagating through the Log4j vulnerability on February 9, 2022, the malware leverages a technique called DNS tunneling to build communication channels with command-and-control (C2) servers by encoding data in DNS queries and responses.  B1txor20, while also buggy in some ways, currently supports the ability to obtain a shell, execute arbitrary commands, install a rootkit, open a SOCKS5 proxy, and functions to upload sensitive information back to the C2 server. Once a machine is successfully compromised, the malware utilizes the DNS tunnel to retrieve and execute commands sent by the server.  "Bot sends the stolen sensitive information, command execution results, and any other information that needs to be delivered, after hiding it using specific encoding techniques, to C2 as a DNS request," the researchers elaborated. "After receiving the request, C2 sends the payload to the Bot side as a response to the DNS request. In this way, Bot and C2 achieve communication with the help of DNS protocol." A total of 15 commands are implemented, chief among them being uploading system information, executing arbitrary system commands, reading and writing files, starting and stopping proxy services, and creating reverse shells.   Found this article interesting? Follow THN on Facebook, Twitter  and LinkedIn to read more exclusive content we post. | Một cửa hậu không có giấy tờ trước đây đã được quan sát thấy nhắm mục tiêu vào các hệ thống Linux với mục tiêu biến các máy thành một mạng botnet và hoạt động như một đường dẫn để tải xuống và cài đặt rootkit. Nhóm bảo mật Netlab của Qihoo 360 đã gọi nó là B1txor20 "dựa trên sự lan truyền của nó bằng cách sử dụng tên tệp 'b1t', thuật toán mã hóa XOR và độ dài khóa của thuật toán RC4 là 20 byte."  Lần đầu tiên được quan sát thấy sự lan truyền thông qua lỗ hổng Log4j vào ngày 9 tháng 2 năm 2022, phần mềm độc hại này sử dụng một kỹ thuật gọi là đường hầm DNS để xây dựng các kênh giao tiếp với máy chủ lệnh và kiểm soát (C2) bằng cách mã hóa dữ liệu trong các truy vấn và phản hồi DNS.  B1txor20, mặc dù cũng có lỗi ở một số mặt, hiện hỗ trợ khả năng lấy shell, thực hiện các lệnh tùy ý, cài đặt rootkit, mở proxy SOCKS5 và chức năng tải thông tin nhạy cảm trở lại máy chủ C2. Sau khi máy bị xâm nhập thành công, phần mềm độc hại sẽ sử dụng đường hầm DNS để truy xuất và thực thi các lệnh do máy chủ gửi.  Các nhà nghiên cứu giải thích thêm: "Bot gửi thông tin nhạy cảm bị đánh cắp, kết quả thực thi lệnh và bất kỳ thông tin nào khác cần được gửi, sau khi ẩn nó bằng các kỹ thuật mã hóa cụ thể, tới C2 dưới dạng một yêu cầu DNS". "Sau khi nhận được yêu cầu, C2 gửi tải trọng đến phía Bot như một phản hồi đối với yêu cầu DNS. Bằng cách này, Bot và C2 đạt được giao tiếp với sự trợ giúp của giao thức DNS." Tổng cộng có 15 lệnh được thực hiện, chủ yếu trong số đó là tải lên thông tin hệ thống, thực hiện các lệnh hệ thống tùy ý, đọc và ghi tệp, khởi động và dừng các dịch vụ proxy và tạo trình bao ngược.   Tìm thấy bài viết này thú vị? Theo dõi THN trên Facebook, Twitter  và LinkedIn để đọc thêm nội dung độc quyền mà chúng tôi đăng. |

# New Infinite Loop Bug in OpenSSL Could Let Attackers Crash Remote Servers

📅Date: March 16, 2022 👤Author: Ravie Lakshmanan

Link tham khảo: *https://thehackernews.com/2022/03/new-infinite-loop-bug-in-openssl-could.html*



|  |  |
| --- | --- |
| Title: 🐄New Infinite Loop Bug in OpenSSL Could Let Attackers Crash Remote Servers | Title: 🐄Lỗi vòng lặp vô hạn mới trong OpenSSL có thể cho phép kẻ tấn công làm hỏng máy chủ từ xa |
| The maintainers of OpenSSL have shipped patches to resolve a high-severity security flaw in its software library that could lead to a denial-of-service (DoS) condition when parsing certificates. Tracked as CVE-2022-0778 (CVSS score: 7.5), the issue stems from parsing a malformed certificate with invalid explicit elliptic-curve parameters, resulting in what's called an "infinite loop." The flaw resides in a function called BN\_mod\_sqrt() that's used to compute the modular square root.  "Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial-of-service attack," OpenSSL said in an advisory published on March 15, 2022. "The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic-curve parameters." While there is no evidence that the vulnerability has been exploited in the wild, there are a few scenarios where it could be weaponized, including when TLS clients (or servers) access a rogue certificate from a malicious server (or client), or when certificate authorities parse certification requests from subscribers. The vulnerability impacts OpenSSL versions 1.0.2, 1.1.1, and 3.0, the project owners addressed the flaw with the release of versions 1.0.2zd (for premium support customers), 1.1.1n, and 3.0.2. OpenSSL 1.1.0, while also affected, will not receive a fix as it has reached end-of-life.  Credited with reporting the flaw on February 24, 2022 is Google Project Zero security researcher Tavis Ormandy. The fix was developed by David Benjamin from Google and Tomáš Mráz from OpenSSL. CVE-2022-0778 is also the second OpenSSL vulnerability resolved since the start of the year. On January 28, 2022, the maintainers fixed a moderate-severity flaw (CVE-2021-4160, CVSS score: 5.9) affecting the library's MIPS32 and MIPS64 squaring procedure.   Found this article interesting? Follow THN on Facebook, Twitter  and LinkedIn to read more exclusive content we post. | Những người bảo trì OpenSSL đã gửi các bản vá để giải quyết một lỗ hổng bảo mật nghiêm trọng cao trong thư viện phần mềm của nó có thể dẫn đến tình trạng từ chối dịch vụ (DoS) khi phân tích cú pháp chứng chỉ. Được theo dõi là CVE-2022-0778 (điểm CVSS: 7,5), sự cố bắt nguồn từ việc phân tích cú pháp một chứng chỉ không đúng định dạng với các tham số đường cong elliptic rõ ràng không hợp lệ, dẫn đến cái được gọi là "vòng lặp vô hạn". Lỗ hổng nằm trong một hàm có tên BN\_mod\_sqrt () được sử dụng để tính căn bậc hai mô-đun.  "Vì quá trình phân tích cú pháp chứng chỉ xảy ra trước khi xác minh chữ ký chứng chỉ, bất kỳ quá trình nào phân tích cú pháp chứng chỉ được cung cấp bên ngoài do đó có thể bị tấn công từ chối dịch vụ", OpenSSL cho biết trong một tư vấn được công bố vào ngày 15 tháng 3 năm 2022. "Vòng lặp vô hạn cũng có thể đạt được khi phân tích cú pháp các khóa riêng tư được tạo thủ công vì chúng có thể chứa các tham số đường cong elliptic rõ ràng." Mặc dù không có bằng chứng cho thấy lỗ hổng bảo mật đã bị khai thác một cách tự nhiên, nhưng có một số trường hợp mà nó có thể được vũ khí hóa, bao gồm khi máy khách TLS (hoặc máy chủ) truy cập chứng chỉ giả mạo từ một máy chủ độc hại (hoặc máy khách) hoặc khi chứng chỉ cơ quan chức năng phân tích các yêu cầu chứng nhận từ người đăng ký. Lỗ hổng bảo mật ảnh hưởng đến các phiên bản OpenSSL 1.0.2, 1.1.1 và 3.0, chủ dự án đã khắc phục lỗ hổng này bằng việc phát hành các phiên bản 1.0.2zd (dành cho khách hàng hỗ trợ cao cấp), 1.1.1n và 3.0.2. OpenSSL 1.1.0, trong khi cũng bị ảnh hưởng, sẽ không nhận được bản sửa lỗi vì nó đã hết tuổi thọ.  Nhà nghiên cứu bảo mật Tavis Ormandy của Google Project Zero đã báo cáo lỗ hổng vào ngày 24 tháng 2 năm 2022. Bản sửa lỗi được phát triển bởi David Benjamin từ Google và Tomáš Mráz từ OpenSSL. CVE-2022-0778 cũng là lỗ hổng OpenSSL thứ hai được giải quyết kể từ đầu năm. Vào ngày 28 tháng 1 năm 2022, những người bảo trì đã sửa một lỗ hổng ở mức độ trung bình (CVE-2021-4160, điểm CVSS: 5,9) ảnh hưởng đến quy trình bình phương MIPS32 và MIPS64 của thư viện.   Tìm thấy bài viết này thú vị? Theo dõi THN trên Facebook, Twitter  và LinkedIn để đọc thêm nội dung độc quyền mà chúng tôi đăng. |

# FBI, CISA Warn of Russian Hackers Exploiting MFA and PrintNightmare Bug

📅Date: March 16, 2022 👤Author: Ravie Lakshmanan

Link tham khảo: *https://thehackernews.com/2022/03/fbi-cisa-warn-of-russian-hackers.html*

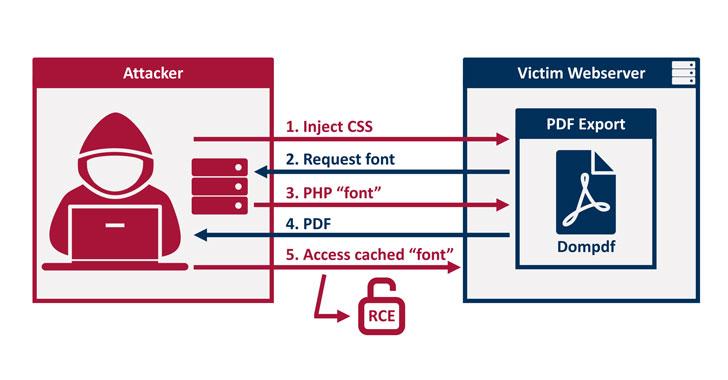


|  |  |
| --- | --- |
| Title: 🐄FBI, CISA Warn of Russian Hackers Exploiting MFA and PrintNightmare Bug | Title: 🐄FBI, CISA Cảnh báo về việc tin tặc Nga khai thác MFA và lỗi PrintNightmare |
| The U.S. Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) have released a joint advisory warning that Russia-backed threat actors hacked the network of an unnamed non-governmental entity by exploiting a combination of flaws. "As early as May 2021, Russian state-sponsored cyber actors took advantage of a misconfigured account set to default [multi-factor authentication] protocols at a non-governmental organization (NGO), allowing them to enroll a new device for MFA and access the victim network," the agencies said.  "The actors then exploited a critical Windows Print Spooler vulnerability, 'PrintNightmare' (CVE-2021-34527) to run arbitrary code with system privileges." The attack was pulled off by gaining initial access to the victim organization via compromised credentials – obtained by means of a brute-force password guessing attack – and enrolling a new device in the organization's Duo MFA. It's also noteworthy that the breached account was un-enrolled from Duo due to a long period of inactivity, but had not yet been disabled in the NGO's Active Directory, thereby allowing the attackers to escalate their privileges using the PrintNightmare flaw and disable the MFA service altogether. "As Duo's default configuration settings allow for the re-enrollment of a new device for dormant accounts, the actors were able to enroll a new device for this account, complete the authentication requirements, and obtain access to the victim network," the agencies explained.  Turning off MFA, in turn, allowed the state-sponsored actors to authenticate to the NGO's virtual private network (VPN) as non-administrator users, connect to Windows domain controllers via Remote Desktop Protocol (RDP), and obtain credentials for other domain accounts. In the final stage of the attack, the newly compromised accounts were subsequently utilized to move laterally across the network to siphon data from the organization's cloud storage and email accounts. To mitigate such attacks, both CISA and FBI are recommending organizations to enforce and review multi-factor authentication configuration policies, disable inactive accounts in Active Directory, and prioritize patching for known exploited flaws.   Found this article interesting? Follow THN on Facebook, Twitter  and LinkedIn to read more exclusive content we post. | Cơ quan An ninh mạng và Cơ sở hạ tầng Hoa Kỳ (CISA) và Cục Điều tra Liên bang (FBI) đã đưa ra một cảnh báo cố vấn chung rằng các kẻ đe dọa do Nga hậu thuẫn đã tấn công mạng của một tổ chức phi chính phủ giấu tên bằng cách khai thác kết hợp các lỗ hổng. "Ngay từ tháng 5 năm 2021, các diễn viên mạng do nhà nước Nga tài trợ đã lợi dụng tài khoản bị định cấu hình sai được đặt thành các giao thức [xác thực đa yếu tố] mặc định tại một tổ chức phi chính phủ (NGO), cho phép họ đăng ký một thiết bị mới cho MFA và truy cập mạng lưới nạn nhân, "các cơ quan cho biết.  "Các tác nhân sau đó đã khai thác một lỗ hổng nghiêm trọng của Windows Print Spooler, 'PrintNightmare' (CVE-2021-34527) để chạy mã tùy ý với các đặc quyền của hệ thống." Cuộc tấn công đã được kết thúc bằng cách giành được quyền truy cập ban đầu vào tổ chức nạn nhân thông qua thông tin đăng nhập bị xâm phạm - có được bằng một cuộc tấn công đoán mật khẩu bạo lực - và đăng ký một thiết bị mới trong Duo MFA của tổ chức. Cũng cần lưu ý rằng tài khoản vi phạm đã được hủy đăng ký Duo do một thời gian dài không hoạt động, nhưng vẫn chưa bị vô hiệu hóa trong Active Directory của tổ chức phi chính phủ, do đó cho phép những kẻ tấn công nâng cao đặc quyền của họ bằng cách sử dụng lỗ hổng PrintNightmare và vô hiệu hóa dịch vụ MFA hoàn toàn. Các cơ quan giải thích: "Do cài đặt cấu hình mặc định của Duo cho phép đăng ký lại thiết bị mới cho tài khoản không hoạt động, nên các diễn viên có thể đăng ký thiết bị mới cho tài khoản này, hoàn thành các yêu cầu xác thực và có quyền truy cập vào mạng nạn nhân" .  Đến lượt nó, việc tắt MFA cho phép các tác nhân do nhà nước tài trợ xác thực với mạng riêng ảo (VPN) của NGO với tư cách là người dùng không phải là quản trị viên, kết nối với bộ điều khiển miền Windows qua Giao thức Máy tính Từ xa (RDP) và lấy thông tin đăng nhập cho các tài khoản miền khác . Trong giai đoạn cuối của cuộc tấn công, các tài khoản mới bị xâm nhập sau đó đã được sử dụng để di chuyển ngang qua mạng nhằm lấy dữ liệu từ các tài khoản email và lưu trữ đám mây của tổ chức. Để giảm thiểu các cuộc tấn công như vậy, cả CISA và FBI đều khuyến nghị các tổ chức thực thi và xem xét các chính sách cấu hình xác thực đa yếu tố, vô hiệu hóa các tài khoản không hoạt động trong Active Directory và ưu tiên vá các lỗi đã khai thác.   Tìm thấy bài viết này thú vị? Theo dõi THN trên Facebook, Twitter  và LinkedIn để đọc thêm nội dung độc quyền mà chúng tôi đăng. |

# Unpatched RCE Bug in dompdf Project Affects HTML to PDF Converters

📅Date: March 16, 2022 👤Author: Ravie Lakshmanan

Link tham khảo: *https://thehackernews.com/2022/03/unpatched-rce-bug-in-dompdf-project.html*



|  |  |
| --- | --- |
| Title: 🐄Unpatched RCE Bug in dompdf Project Affects HTML to PDF Converters | Title: 🐄Lỗi RCE chưa được khắc phục trong dự án dompdf ảnh hưởng đến trình chuyển đổi HTML sang PDF |
| Researchers have disclosed an unpatched security vulnerability in "dompdf," a PHP-based HTML to PDF converter, that, if successfully exploited, could lead to remote code execution in certain configurations. "By injecting CSS into the data processed by dompdf, it can be tricked into storing a malicious font with a .php file extension in its font cache, which can later be executed by accessing it from the web," Positive Security researchers Maximilian Kirchmeier and Fabian Bräunlein said in a report published today.  In other words, the flaw allows a malicious party to upload font files with a .php extension to the web server, which can then be activated by using an XSS vulnerability to inject HTML into a web page before it's rendered as a PDF.  This meant that the attacker could potentially navigate to the uploaded .php script, effectively permitting remote code execution on the server. This can have significant consequences on websites that require server-side generation of PDFs based on user-supplied data, such as ticket purchases and other receipts, particularly when inputs are not adequately sanitized to mitigate XSS flaws or if the library is installed in a publicly-accessible directory. According to statistics on GitHub, dompdf is used in nearly 59,250 repositories, making it a popular library for generating PDFs in the PHP programming language.  Dompdf versions 1.2.0 and prior that are located in a web-accessible directory and have the setting "$isRemoteEnabled" toggled on should be considered vulnerable. Versions 0.8.5 and before of the library, however, are impacted even when this option is set to false. Although the vulnerability was reported to the open-source project maintainers on October 5, 2021, the developers are yet to provide a timeline by when the fixes are expected to be rolled out. "Security vulnerabilities often occur due to (design) decisions made based on incorrect assumptions about underlying or interconnected components," the researchers said. "Update dompdf to a recent version and turn off $isRemoteEnabled, if possible for your use case."   Found this article interesting? Follow THN on Facebook, Twitter  and LinkedIn to read more exclusive content we post. | Các nhà nghiên cứu đã tiết lộ một lỗ hổng bảo mật chưa được vá trong "dompdf", một công cụ chuyển đổi HTML sang PDF dựa trên PHP, nếu khai thác thành công, có thể dẫn đến thực thi mã từ xa trong một số cấu hình nhất định. Nhà nghiên cứu Maximilian Kirchmeier của Positive Security và Fabian Bräunlein cho biết trong một báo cáo được công bố ngày hôm nay.  Nói cách khác, lỗ hổng này cho phép một bên độc hại tải các tệp phông chữ có phần mở rộng .php lên máy chủ web, sau đó có thể được kích hoạt bằng cách sử dụng lỗ hổng XSS để đưa HTML vào một trang web trước khi nó được hiển thị dưới dạng PDF.  Điều này có nghĩa là kẻ tấn công có thể điều hướng đến tập lệnh .php được tải lên, cho phép thực thi mã từ xa trên máy chủ một cách hiệu quả. Điều này có thể gây ra hậu quả đáng kể trên các trang web yêu cầu tạo tệp PDF từ phía máy chủ dựa trên dữ liệu do người dùng cung cấp, chẳng hạn như giao dịch mua vé và các biên lai khác, đặc biệt khi đầu vào không được vệ sinh đầy đủ để giảm thiểu lỗi XSS hoặc nếu thư viện được cài đặt công khai -thư mục có thể truy cập. Theo thống kê trên GitHub, dompdf được sử dụng trong gần 59.250 kho, trở thành thư viện phổ biến để tạo PDF bằng ngôn ngữ lập trình PHP.  Dompdf phiên bản 1.2.0 trở về trước nằm trong thư mục có thể truy cập web và có bật cài đặt "$ isRemoteEnabled" nên được coi là dễ bị tấn công. Tuy nhiên, các phiên bản 0.8.5 trở về trước của thư viện sẽ bị ảnh hưởng ngay cả khi tùy chọn này được đặt thành false. Mặc dù lỗ hổng bảo mật đã được báo cáo cho những người bảo trì dự án nguồn mở vào ngày 5 tháng 10 năm 2021, nhưng các nhà phát triển vẫn chưa đưa ra lịch trình về thời điểm các bản sửa lỗi dự kiến ​​sẽ được triển khai. Các nhà nghiên cứu cho biết: “Các lỗ hổng bảo mật thường xảy ra do các quyết định (thiết kế) được đưa ra dựa trên các giả định không chính xác về các thành phần cơ bản hoặc được kết nối với nhau. "Cập nhật dompdf lên phiên bản gần đây và tắt $ isRemoteEnabled, nếu có thể cho trường hợp sử dụng của bạn."   Tìm thấy bài viết này thú vị? Theo dõi THN trên Facebook, Twitter  và LinkedIn để đọc thêm nội dung độc quyền mà chúng tôi đăng. |

# German Government Warns Against Using Russia's Kaspersky Antivirus Software

📅Date: March 16, 2022 👤Author: Ravie Lakshmanan

Link tham khảo: *https://thehackernews.com/2022/03/german-government-warns-against-using.html*



|  |  |
| --- | --- |
| Title: 🐄German Government Warns Against Using Russia's Kaspersky Antivirus Software | Title: 🐄Chính phủ Đức cảnh báo chống lại việc sử dụng phần mềm chống vi-rút Kaspersky của Nga |
| Russian cybersecurity firm Kaspersky on Tuesday responded to an advisory released by Germany's Federal Office of Information Security (BSI) against using the company's security solutions in the country over "doubts about the reliability of the manufacturer." Calling that the decision was made on "political grounds," the company said it will "continue to assure our partners and customers of the quality and integrity of our products, and we will be working with the BSI for clarification on its decision and for the means to address its and other regulators' concerns."  The statement from Kaspersky follows a warning from Germany's cybersecurity authority, the Bundesamt für Sicherheit in der Informationstechnik aka BSI, which recommended "replacing applications from Kaspersky's portfolio of antivirus software with alternative products" due to risks that they could be exploited by Russia for a cyber attack. "Companies and authorities with special security interests and operators of critical infrastructures are particularly at risk," the BSI said, adding the company's tools could be used for attacks against its own customers or be compelled to strike systems against its will amidst Russia's military invasion of Ukraine. Although not an outright ban, the announcement adds to similar restrictions put in place by the U.S., U.K., and Dutch governments in 2017 and 2018 to phase out the use of antivirus software made by Kaspersky Labs.  The Moscow-based company, however, noted that it had shifted its cyberthreat-related data processing infrastructure to the Swiss city of Zurich in 2018 and that its data services and engineering practices have been subjected to independent third-party assessments. Earlier this month, Eugene Kaspersky, CEO of the namesake company, struck a neutral tone, hoping that negotiations between Ukraine and Russia would lead to "a compromise," in an attempt to distance the organization from being branded as siding with Russia. "We believe that peaceful dialogue is the only possible instrument for resolving conflicts," Kaspersky tweeted on March 1. "War isn't good for anyone."   Found this article interesting? Follow THN on Facebook, Twitter  and LinkedIn to read more exclusive content we post. | Công ty an ninh mạng Kaspersky của Nga hôm thứ Ba đã phản hồi một lời khuyên do Văn phòng An ninh Thông tin Liên bang (BSI) của Đức đưa ra về việc sử dụng các giải pháp bảo mật của công ty trong nước vì "nghi ngờ về độ tin cậy của nhà sản xuất." Gọi rằng quyết định được đưa ra trên "cơ sở chính trị", công ty cho biết họ sẽ "tiếp tục đảm bảo với các đối tác và khách hàng của chúng tôi về chất lượng và tính toàn vẹn của sản phẩm của chúng tôi, và chúng tôi sẽ làm việc với BSI để làm rõ về quyết định của họ và có nghĩa là để giải quyết các mối quan tâm của nó và các cơ quan quản lý khác. "  Tuyên bố từ Kaspersky sau cảnh báo từ cơ quan an ninh mạng của Đức, Bundesamt für Sicherheit in der Informationstechnik hay còn gọi là BSI, khuyến nghị "thay thế các ứng dụng từ danh mục phần mềm chống vi-rút của Kaspersky bằng các sản phẩm thay thế" do rủi ro rằng chúng có thể bị Nga khai thác trên mạng tấn công. BSI cho biết: “Các công ty và chính quyền có lợi ích bảo mật đặc biệt và các nhà khai thác cơ sở hạ tầng quan trọng đặc biệt gặp rủi ro,” BSI cho biết, đồng thời cho biết thêm các công cụ của công ty có thể được sử dụng để tấn công các khách hàng của chính họ hoặc bị buộc phải tấn công các hệ thống chống lại ý muốn của họ trong bối cảnh quân đội Nga xâm lược. Ukraina. Mặc dù không phải là lệnh cấm hoàn toàn, nhưng thông báo này bổ sung thêm các hạn chế tương tự do chính phủ Hoa Kỳ, Vương quốc Anh và Hà Lan đưa ra vào năm 2017 và 2018 nhằm loại bỏ dần việc sử dụng phần mềm chống vi-rút do Kaspersky Labs thực hiện.  Tuy nhiên, công ty có trụ sở tại Moscow lưu ý rằng họ đã chuyển cơ sở hạ tầng xử lý dữ liệu liên quan đến đe dọa mạng đến thành phố Zurich của Thụy Sĩ vào năm 2018 và các dịch vụ dữ liệu cũng như hoạt động kỹ thuật của họ đã phải chịu sự đánh giá của bên thứ ba độc lập. Đầu tháng này, Eugene Kaspersky, Giám đốc điều hành của công ty trùng tên, đã đưa ra quan điểm trung lập, hy vọng rằng các cuộc đàm phán giữa Ukraine và Nga sẽ dẫn đến "một thỏa hiệp", trong một nỗ lực nhằm ngăn cách tổ chức được coi là đứng về phía Nga. "Chúng tôi tin rằng đối thoại hòa bình là công cụ khả thi duy nhất để giải quyết xung đột", Kaspersky đã tweet vào ngày 1 tháng 3. "Chiến tranh không tốt cho bất kỳ ai."   Tìm thấy bài viết này thú vị? Theo dõi THN trên Facebook, Twitter  và LinkedIn để đọc thêm nội dung độc quyền mà chúng tôi đăng. |

# Build Your 2022 Cybersecurity Plan With This Free PPT Template

📅Date: March 16, 2022 👤Author: The Hacker News

Link tham khảo: *https://thehackernews.com/2019/11/cybersecurity-plan-template.html*



|  |  |
| --- | --- |
| Title: 🐄Build Your 2022 Cybersecurity Plan With This Free PPT Template | Title: 🐄Xây dựng kế hoạch an ninh mạng năm 2022 của bạn với mẫu PPT miễn phí này |
| The end of the year is coming, and it's time for security decision-makers to make plans for 2022 and get management approval. Typically, this entails making a solid case regarding why current resources, while yielding significant value, need to be reallocated and enhanced.  The Definitive 2022 Security Plan PPT Template is built to simplify this task, providing security decision-makers with an off-the-shelf tool to clearly and easily present their plans and insights to management.  While many security decision-makers have the tools and expertise to build their case technologically, effectively communicating their conclusions to the organization's management is a different challenge.  Management doesn't think in terms of malware, identity compromise, or zero-day exploits, but in terms of monetary loss and gain: Would investment A in a security product reduce the likelihood of cyberattack derived downtime? Would outsourcing a certain security functionality to a service provider optimize the productivity of the in-house team?  If you're the one accountable for security in your organization, you must be able to provide simple answers to these questions.  A significant part of this relates to the pros and cons of the current security posture. What was achieved in the passing year didn't happen by chance but was the result of executing a well-defined strategy. Communicating this strategy and its results are paramount to justifying resource reallocation.  As a rule of thumb, the more you are able to approximate your insights into absolute black and white terms, the better. In other words, if you want to make a case for enlarging the budget to enable the purchase and deployment of new security technology, the management-bound argument shouldn't be its ability to pinpoint malicious behavior more efficiently than the technology currently in place, but it's ability to prevent the direct and implicit monetary loss your organization suffered from a cyberattack over the past year.  While these two arguments seem identical to the security practitioner, they are tremendously different in their ability to capture the mindset of non-security-savvy management.  The Definitive 2022 Security Plan PPT template enables security pros – CISOs, CIOs, security directors, and others – to easily distill their security knowledge and present the insights and conclusions that speak the management language.  The template was built based on feedback from both security stakeholders and management personnel, encompassing the key aspects of presenting an annual plan. Instead of spending valuable time on building their case from scratch, security decision-makers can start from a given infrastructure and focus on filling it in based on their specific needs.  The template consists of three integrated parts:   Overview of the existing allocation of resources for cybersecurity. This includes implemented technologies in place, the cost of the security team (or of the portion of time IT personnel dedicate to cybersecurity-related tasks), and engagement with 3rd party providers, either on an ongoing basis or per specific event.  Evaluation of the cybersecurity performance under the existing resource allocations. On the success side, it would include indications of attacks that have been prevented or efficiently contained by the products and the security team, together with analysis of the potential damage that was eliminated. On the challenge side, it would include cyberattacks that have caused tangible damage to the organization due to a lack of sufficient technology or security team capacity. Future annual planning that takes the evaluation bottom line and translates it into actionable steps. These may include changes in resource allocation, enlarging the security budget, decisions to add or replace security products, decisions to withdraw from or engage with a security service provider, and any other action that would enhance the security posture to address the gaps that were unveiled in during the evaluation.    As you see, the underlying theme of the template is cost. How much did the organization spend on cybersecurity, how much did this spending pay off in the long run, and how much did the organization lose due to an under fitted security budget.  The 2022 Security Plan PPT template is the ideal tool to engage your management and get their approval for your decisions regarding the best security strategy to implement.  Download the Definitive 2022 Security Plan PPT template here.   Found this article interesting? Follow THN on Facebook, Twitter  and LinkedIn to read more exclusive content we post. | Cuối năm sắp đến và đã đến lúc các nhà ra quyết định bảo mật lên kế hoạch cho năm 2022 và nhận được sự chấp thuận của ban quản lý. Thông thường, điều này đòi hỏi phải đưa ra một trường hợp chắc chắn về lý do tại sao các nguồn lực hiện tại, mặc dù mang lại giá trị đáng kể, cần được phân bổ lại và nâng cao.  Mẫu PPT kế hoạch bảo mật Definitive 2022 được xây dựng để đơn giản hóa nhiệm vụ này, cung cấp cho những người ra quyết định bảo mật một công cụ hữu ích để trình bày rõ ràng và dễ dàng các kế hoạch và thông tin chi tiết của họ cho ban quản lý.  Mặc dù nhiều người ra quyết định bảo mật có các công cụ và chuyên môn để xây dựng trường hợp của họ về mặt công nghệ, nhưng việc truyền đạt hiệu quả kết luận của họ cho ban quản lý của tổ chức là một thách thức khác.  Ban quản lý không nghĩ về phần mềm độc hại, xâm phạm danh tính hoặc khai thác zero-day, mà xét về tổn thất và lợi nhuận về tiền tệ: Liệu khoản đầu tư A vào một sản phẩm bảo mật có làm giảm khả năng bị tấn công mạng do thời gian ngừng hoạt động không? Việc thuê ngoài một chức năng bảo mật nhất định cho nhà cung cấp dịch vụ có tối ưu hóa năng suất của nhóm nội bộ không?  Nếu bạn là người chịu trách nhiệm về bảo mật trong tổ chức của mình, bạn phải có khả năng đưa ra câu trả lời đơn giản cho những câu hỏi này.  Một phần quan trọng của điều này liên quan đến ưu và nhược điểm của thế trận an ninh hiện tại. Những gì đạt được trong năm qua không phải do ngẫu nhiên mà là kết quả của việc thực hiện một chiến lược được xác định rõ ràng. Việc truyền đạt chiến lược này và kết quả của nó là điều tối quan trọng để biện minh cho việc phân bổ lại nguồn lực.  Theo nguyên tắc chung, bạn càng có nhiều khả năng gần đúng những hiểu biết của mình về các thuật ngữ đen trắng tuyệt đối thì càng tốt. Nói cách khác, nếu bạn muốn mở rộng ngân sách để cho phép mua và triển khai công nghệ bảo mật mới, lập luận ràng buộc quản lý không nên là khả năng xác định hành vi độc hại hiệu quả hơn công nghệ hiện tại, nhưng nó có khả năng ngăn chặn tổn thất tiền tệ trực tiếp và tiềm ẩn mà tổ chức của bạn phải chịu đựng bởi một cuộc tấn công mạng trong năm qua.  Mặc dù hai lập luận này có vẻ giống hệt nhau về chuyên gia bảo mật, nhưng chúng rất khác nhau về khả năng nắm bắt tư duy của quản lý không am hiểu về bảo mật.  Mẫu PPT của Kế hoạch bảo mật cuối cùng năm 2022 cho phép các chuyên gia bảo mật - CISO, CIO, giám đốc bảo mật và những người khác - dễ dàng chắt lọc kiến ​​thức bảo mật của họ và trình bày những hiểu biết sâu sắc và kết luận bằng ngôn ngữ quản lý.  Mẫu được xây dựng dựa trên phản hồi từ cả các bên liên quan đến bảo mật và nhân viên quản lý, bao gồm các khía cạnh chính của việc trình bày kế hoạch hàng năm. Thay vì dành thời gian quý báu để xây dựng trường hợp của họ từ đầu, những người ra quyết định bảo mật có thể bắt đầu từ một cơ sở hạ tầng nhất định và tập trung vào việc lấp đầy nó dựa trên nhu cầu cụ thể của họ.  Mẫu bao gồm ba phần tích hợp:   Tổng quan về việc phân bổ các nguồn lực hiện có cho an ninh mạng. Điều này bao gồm các công nghệ được triển khai tại chỗ, chi phí của đội bảo mật (hoặc phần thời gian mà nhân viên CNTT dành cho các nhiệm vụ liên quan đến an ninh mạng) và sự tham gia với các nhà cung cấp bên thứ ba, trên cơ sở liên tục hoặc cho mỗi sự kiện cụ thể.  Đánh giá hiệu suất an ninh mạng theo phân bổ tài nguyên hiện có. Về mặt thành công, nó sẽ bao gồm các dấu hiệu về các cuộc tấn công đã được các sản phẩm và nhóm bảo mật ngăn chặn hoặc ngăn chặn một cách hiệu quả, cùng với phân tích về thiệt hại tiềm ẩn đã được loại bỏ. Về mặt thách thức, nó sẽ bao gồm các cuộc tấn công mạng đã gây ra thiệt hại hữu hình cho tổ chức do thiếu công nghệ hoặc năng lực của đội bảo mật. Lập kế hoạch hàng năm trong tương lai lấy điểm mấu chốt của việc đánh giá và chuyển nó thành các bước có thể hành động được. Những điều này có thể bao gồm những thay đổi trong phân bổ nguồn lực, mở rộng ngân sách bảo mật, quyết định thêm hoặc thay thế các sản phẩm bảo mật, quyết định rút khỏi hoặc tham gia với nhà cung cấp dịch vụ bảo mật và bất kỳ hành động nào khác có thể nâng cao thế trận an ninh để giải quyết những lỗ hổng đã được tiết lộ trong quá trình đánh giá.   Như bạn thấy, chủ đề cơ bản của mẫu là chi phí. Tổ chức đã chi bao nhiêu cho an ninh mạng, khoản chi này mang lại lợi nhuận bao nhiêu về lâu dài, và tổ chức đã mất bao nhiêu do ngân sách an ninh chưa được trang bị đầy đủ.  Mẫu PPT của Kế hoạch Bảo mật năm 2022 là công cụ lý tưởng để thu hút sự tham gia của ban quản lý và nhận được sự chấp thuận của họ đối với các quyết định của bạn về chiến lược bảo mật tốt nhất để thực hiện.  Tải xuống mẫu PPT kế hoạch bảo mật cuối cùng 2022 tại đây.   Tìm thấy bài viết này thú vị? Theo dõi THN trên Facebook, Twitter  và LinkedIn để đọc thêm nội dung độc quyền mà chúng tôi đăng. |

# Multiple Flaws Uncovered in ClickHouse OLAP Database System for Big Data

📅Date: March 16, 2022 👤Author: Ravie Lakshmanan

Link tham khảo: *https://thehackernews.com/2022/03/multiple-flaws-uncovered-in-clickhouse.html*



|  |  |
| --- | --- |
| Title: 🐄Multiple Flaws Uncovered in ClickHouse OLAP Database System for Big Data | Title: 🐄Nhiều Flaws được phát hiện trong Hệ thống cơ sở dữ liệu ClickHouse OLAP cho Dữ liệu lớn |
| Researchers have disclosed seven new security vulnerabilities in an open-source database management system solution called ClickHouse that could be weaponized to crash the servers, leak memory contents, and even lead to the execution of arbitrary code. "The vulnerabilities require authentication, but can be triggered by any user with read permissions," Uriya Yavnieli and Or Peles, researchers from DevSecOps firm JFrog, said in a report published Tuesday. "This means the attacker must perform reconnaissance on the specific ClickHouse server target to obtain valid credentials. Any set of credentials would do, since even a user with the lowest privileges can trigger all of the vulnerabilities."  The list of seven flaws is below –  CVE-2021-43304 and CVE-2021-43305 (CVSS scores: 8.8) – Heap buffer overflow flaws in the LZ4 compression codec that could lead to remote code execution CVE-2021-42387 and CVE-2021-42388 (CVSS scores: 7.1) – Heap out-of-bounds read flaws in the LZ4 compression codec that could lead to denial-of-service or information leakage CVE-2021-42389 (CVSS score: 6.5) – A divide-by-zero flaw in the Delta compression codec that could result in a denial-of-service condition CVE-2021-42390 (CVSS score: 6.5) – A divide-by-zero flaw in the DeltaDouble compression codec that could result in a denial-of-service condition CVE-2021-42391 (CVSS score: 6.5) – A divide-by-zero flaw in the Gorilla compression codec that could result in a denial-of-service condition   An attacker can take advantage of any of the aforementioned flaws by using a specially crafted compressed file to crash a vulnerable database server. ClickHouse users are recommended to upgrade to version "v21.10.2.15-stable" or later to mitigate the issues. The findings come a month after JFrog disclosed details of a high-severity security vulnerability in Apache Cassandra (CVE-2021-44521, CVSS score: 8.4) that, if left unaddressed, could be abused to gain remote code execution (RCE) on affected installations.   Found this article interesting? Follow THN on Facebook, Twitter  and LinkedIn to read more exclusive content we post. | Các nhà nghiên cứu đã tiết lộ bảy lỗ hổng bảo mật mới trong một giải pháp hệ thống quản lý cơ sở dữ liệu mã nguồn mở có tên ClickHouse có thể được vũ khí hóa để làm hỏng máy chủ, rò rỉ nội dung bộ nhớ và thậm chí dẫn đến việc thực thi mã tùy ý. "Các lỗ hổng yêu cầu xác thực, nhưng có thể được kích hoạt bởi bất kỳ người dùng nào có quyền đọc", Uriya Yavnieli và Or Peles, các nhà nghiên cứu từ công ty DevSecOps JFrog, cho biết trong một báo cáo được công bố hôm thứ Ba. "Điều này có nghĩa là kẻ tấn công phải thực hiện do thám mục tiêu máy chủ ClickHouse cụ thể để có được thông tin xác thực hợp lệ. Bất kỳ bộ thông tin xác thực nào cũng được, vì ngay cả người dùng có đặc quyền thấp nhất cũng có thể kích hoạt tất cả các lỗ hổng."  Dưới đây là danh sách bảy sai sót -  CVE-2021-43304 và CVE-2021-43305 (Điểm CVSS: 8,8) - Lỗ hổng tràn bộ đệm đống trong codec nén LZ4 có thể dẫn đến thực thi mã từ xa CVE-2021-42387 và CVE-2021-42388 (Điểm CVSS: 7,1) - Đống lỗi đọc ngoài giới hạn trong codec nén LZ4 có thể dẫn đến từ chối dịch vụ hoặc rò rỉ thông tin CVE-2021-42389 (Điểm CVSS: 6,5) - Một lỗ hổng chia cho không trong codec nén Delta có thể dẫn đến tình trạng từ chối dịch vụ CVE-2021-42390 (Điểm CVSS: 6,5) - Một lỗ hổng chia cho không trong codec nén DeltaDouble có thể dẫn đến tình trạng từ chối dịch vụ CVE-2021-42391 (Điểm CVSS: 6,5) - Một lỗ hổng chia cho 0 trong codec nén Gorilla có thể dẫn đến tình trạng từ chối dịch vụ   Kẻ tấn công có thể lợi dụng bất kỳ lỗ hổng nào nói trên bằng cách sử dụng một tệp nén được chế tạo đặc biệt để làm sập một máy chủ cơ sở dữ liệu dễ bị tấn công. Người dùng ClickHouse nên nâng cấp lên phiên bản "v21.10.2.15-ổn định" hoặc mới hơn để giảm thiểu sự cố. Phát hiện được đưa ra một tháng sau khi JFrog tiết lộ chi tiết về lỗ hổng bảo mật mức độ nghiêm trọng cao trong Apache Cassandra (CVE-2021-44521, điểm CVSS: 8,4) mà nếu không được giải quyết, có thể bị lạm dụng để thực thi mã từ xa (RCE) khi bị ảnh hưởng cài đặt.   Tìm thấy bài viết này thú vị? Theo dõi THN trên Facebook, Twitter  và LinkedIn để đọc thêm nội dung độc quyền mà chúng tôi đăng. |