**Tin tặc khai thác lỗ hổng PHP để triển khai Backdoor Msupedge ẩn**

https://thehackernews.com/2024/08/hackers-exploit-php-vulnerability-to.html

Backdoor chưa được ghi nhận trước đây, có tên là Msupedge, đã được sử dụng trong một cuộc t.ấn c.ông mạng nhằm vào một trường đại học ở Đài Loan.

Điểm nổi bật của Msupedge

Theo báo cáo từ Đội Ngũ Phân Tích Mối Đe Dọa của Symantec (thuộc Broadcom) được chia sẻ với The Hacker News, Msupedge có một tính năng đáng chú ý: nó giao tiếp với máy chủ chỉ huy và kiểm soát (C&C) thông qua lưu lượng DNS. Điều này có nghĩa là Msupedge sử dụng các yêu cầu DNS để nhận lệnh từ máy chủ C&C.

Nguồn gốc của Msupedge và mục tiêu của cuộc t.ấn côn.g vẫn chưa được biết rõ. Tuy nhiên, có khả năng Msupedge được triển khai thông qua việc khai thác một lỗ hổng PHP nghiêm trọng mới được công bố (CVE-2024-4577, điểm CVSS: 9.8), có thể cho phép thực thi mã từ xa.

Msupedge

Backdoor này là một thư viện liên kết động (DLL) được cài đặt tại các đường dẫn "csidl\_drive\_fixed\xampp\" và "csidl\_system\wbem\". Một trong các DLL, wuplog.dll, được khởi chạy bởi máy chủ HTTP Apache (httpd). Quy trình cha của DLL còn lại chưa được xác định.

Điểm nổi bật của Msupedge là việc nó sử dụng tunneling DNS để giao tiếp với máy chủ C&C, với mã dựa trên công cụ mã nguồn mở dnscat2.

Cách hoạt động của Msupedge

Nhận Lệnh Qua DNS: Msupedge nhận lệnh bằng cách thực hiện phân giải tên miền. Địa chỉ IP của máy chủ C&C (ctl.msedeapi[.]net) được sử dụng như một lệnh.

Chuyển Đổi Địa Chỉ IP: Octet thứ ba của địa chỉ IP đã phân giải hoạt động như một công tắc, xác định hành vi của backdoor bằng cách trừ bảy và sử dụng ký hiệu hexa để kích hoạt phản hồi tương ứng.

Các lệnh hỗ trợ bởi Msupedge bao gồm:

0x8a: Tạo một quy trình sử dụng lệnh nhận được qua bản ghi DNS TXT.

0x75: Tải xuống tệp từ URL tải xuống nhận được qua bản ghi DNS TXT.

0x24: Ngủ trong một khoảng thời gian đã xác định.

0x66: Ngủ trong một khoảng thời gian đã xác định.

0x38: Tạo một tệp tạm thời "%temp%\1e5bf625-1678-zzcv-90b1-199aa47c345.tmp" với mục đích chưa rõ.

0x3c: Xóa tệp "%temp%\1e5bf625-1678-zzcv-90b1-199aa47c345.tmp".

Đồng thời, nhóm đe dọa UTG-Q-010 đã được liên kết với một chiến dịch l.ừa đả.o mới, sử dụng các chiêu trò liên quan đến tiền điện tử và công việc để phân phối phần mềm độc hại mã nguồn mở gọi là Pupy RAT.

***Chuỗi tấn công***

Tệp .lnk độc hại với một trình tải DLL nhúng, dẫn đến việc triển khai payload Pupy RAT.

Pupy RAT là một Trojan Truy Cập Từ Xa (RAT) dựa trên Python với các chức năng như tải DLL phản chiếu và thực thi trong bộ nhớ.

***Khuyến cáo***

Các tổ chức và người dùng nên nhanh chóng cập nhật các bản vá bảo mật và kiểm tra các hệ thống của mình để phát hiện bất kỳ dấu hiệu nào của các cuộc tấn công tương tự.