هشدار در خصوص افزایش حملات به سرویس SMB (درگاه ۴۴۵)

پیرو اطلاعیه قبلی درخصوص وجود آسیب‌پذیری سرویس SMB (درگاه ۴۴۵) در سطح کشور، بررسی‌های انجام شده نشان‌دهنده افزایش سطح حملات روی این درگاه است. این درگاه به صورت پیش‌فرض در پروتکل SMB مورد استفاده قرار می‌گیرد که در گذشته مورد هجوم حملات بسیاری بوده است. آنچه در این ارتباط مورد توجه است، افزایش حملات در سطح کشور از مبدا داخل ایران است که می‌تواند گویای افزایش آلودگی در کشور باشد. از این رو لازم است تا پاکسازی سیستم‌های آلوده داخلی مورد توجه قرار گیرد. خلاصه‌ای از وضعیت حملات ثبت شده از ابتدای مهر به شرح زیر است:

خلاصه وضعیت حملات شناسایی شده توسط سامانه ملی هانی نت از ابتدای مهرماه		
اطلاعات	جهان	ایران
تعداد حملات	۷۱۸۸٤۳	۱۰۳٤٤۲
تعداد آدرس های مهاجم آلوده	٥۹۸۸٥	۲۷۹۸
تعداد بدافزارها	۳۰٤۳	۲٦۳
تعداد کشور مهاجم	۱٥۹	۱
درصد از کل حملات ثبت شده به سرویس SMB	۸٥.٦۱	۱٤.۳۹

لازم به ذکر است بر اساس گزارش منتشر شده از کسپرسکی اخیرا گروه shadow broker ابزاری با نام DarkPulsar را ارائه کرده‌اند که با بهره‌گیری از این آسیب‌پذیری، اجازه کنترل راه‌دور را برای مهاجم فراهم می‌کند. علاوه بر آن دو چارچوب پیچیده دیگر با نام‌های DanderSpritz و FuzzBunch نیز توسط این گروه در سال ۲۰۱۷ ارائه شده است که دارای قابلیت تحلیل میزبان قربانی، آسیب‌پذیری‌های قابل اکسپلویت و سایر مولفه‌های مانیتور میزبان قربانی هستند. ابزار DarkPulsar در زمان اکسپلویت میزبان قربانی عمل کرده و از طریق فعال کردن یک درپشتی به نام sipauth۳۲.tsp فرصت کنترل راه دور را فراهم می‌کند. مهاجمین از این طریق دو سیستم‌عامل سرور ۲۰۰۳ و ۲۰۰۸ را هدف قرار داده‌اند که عمدتا متعلق به سازمان‌های انرژی هسته‌ای، مخابرات، هوا - فضا و پژوهشگاه‌های تحقیق و توسعه در کشورهای روسیه، ایران و مصر می‌باشند. تاکنون ۵۰ قربانی در این کشورها شناسایی شده است. تحلیلگران این حملات بر این باورند که با توجه به داشتن چارچوب‌های قدرتمند تحلیل توسط مهاجمین، آنها پس از اتمام حملات خود، بدافزارهای منتشر شده را پاکسازی خواهند کرد.

محققین بر این باورند که DarkPulsar به دنبال کنترل فرایندهای تصدیق اصالت مبتنی بر پروتکل‌های زیر است:

- Msv۱_۰.dll – for the NTLM protocol
- Kerberos.dll – for the Kerberos protocol
- Schannel.dll – for the TLS/SSL protocols
- Wdigest.dll – for the Digest protocol
- Lsasrv.dll –for the Negotiate protocol

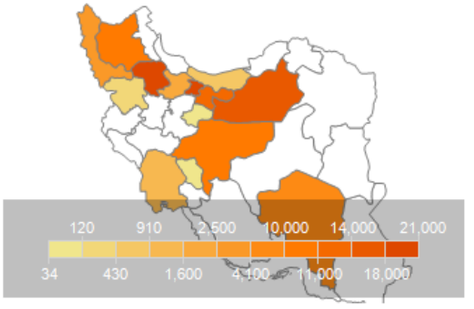
در صورت موفقیت مهاجم، وی می‌تواند بدافزار خود را در پروتکل‌های سیستم قربانی تعبیه کند. در نتیجه وی می‌تواند بدون ورود اطلاعات صحیح تصدیق اصالت، به اطلاعات مورد نیاز خود دست یابد. از جمله مواردی که می‌تواند بدون تصدیق اصالت به آن دست‌یابد شامل لیست فرایندها، رجیسترهای راه‌دور و فایل سیستم از طریق SMB است. نوع بدافزار مورد استفاده در این حملات ناشناخته است ولی با توجه به آنکه دسترسی راه دور برای مهاجم فراهم می‌شود، وی می‌تواند هر نوع بدافزاری را اجرا کند.

در این مقطع مناسب است برای رفع آلودگی برخی از آدرس‌های آلوده و همچنین امن‌سازی سرویس SMB اقدامات مقتضی صورت گیرد.

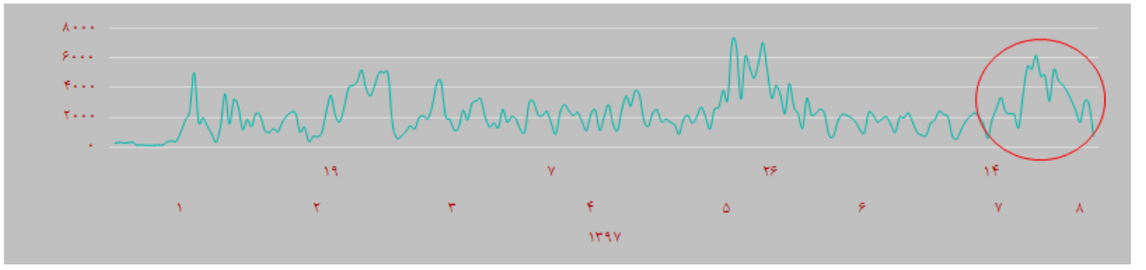
وضعیت حملات ایران از ابتدای مهر

مبدا حملات

مقصد حملات از ایران



روند حملات از ایران



بدافزارهای برتر از ایران

بدافزار	تعداد
8a4e9f688c6d0effd0fa17461352ed3e	4090
cbd91d483bc5d87b16938163e75ef67f	3609
24899e33d1f6f7d1dbb4ecb458c4f057	3349
37a98c6150d2317eb6e0df1516a5b3a4	1867
ca71f8a79f8ed255bf03679504813c6a	1618
0ab2aeda90221832167e5127332dd702	1293
474ecb2fac7ef6f1b798d81d8a3ba5a2	1236
6e72ad805b4322612b9c9c7673a45635	471

آدرس‌های برتر مهاجم از ایران

آدرس	کشور	تعداد
37.152.*.*	ایران	5380
185.83. *.*	ایران	4404
46.32. *.*	ایران	4399
78.38. *.*	ایران	2951
91.243. *.*	ایران	2323
78.38. *.*	ایران	1978
78.38. *.*	ایران	1967
31.25. *.*	ایران	1817