ماهنامه اداره کل پدافند غیرعامل
شماره ۷۱/ مرداد ماه ۱۴۰۱

ماهنامه دیجیتالی پدافند غیرعامل

با حکم استاندار؛
مدیرکل پدافند غیرعامل استانداری آذربایجان شرقی منصوب شد

مدیرکل پدافند غیرعامل استانداری؛
بر رعایت الزامات، ملاحظات و اسناد بالادستی و پیش بینی و پیشگیری از موارد مربوطه از منظر پدافند غیرعامل و همچنین استفاده از نیروهای جوان و متعهد، مدیریت میدانی و کارهای تیمی و تخصصی تأکید نمود

در این شماره می‌خوانید:

جهت دسترسی به آرشیو نشریه به این لینک مراجعه فرمایید.

بسم الله الرحمن الرحیم

فهرست مطالب:

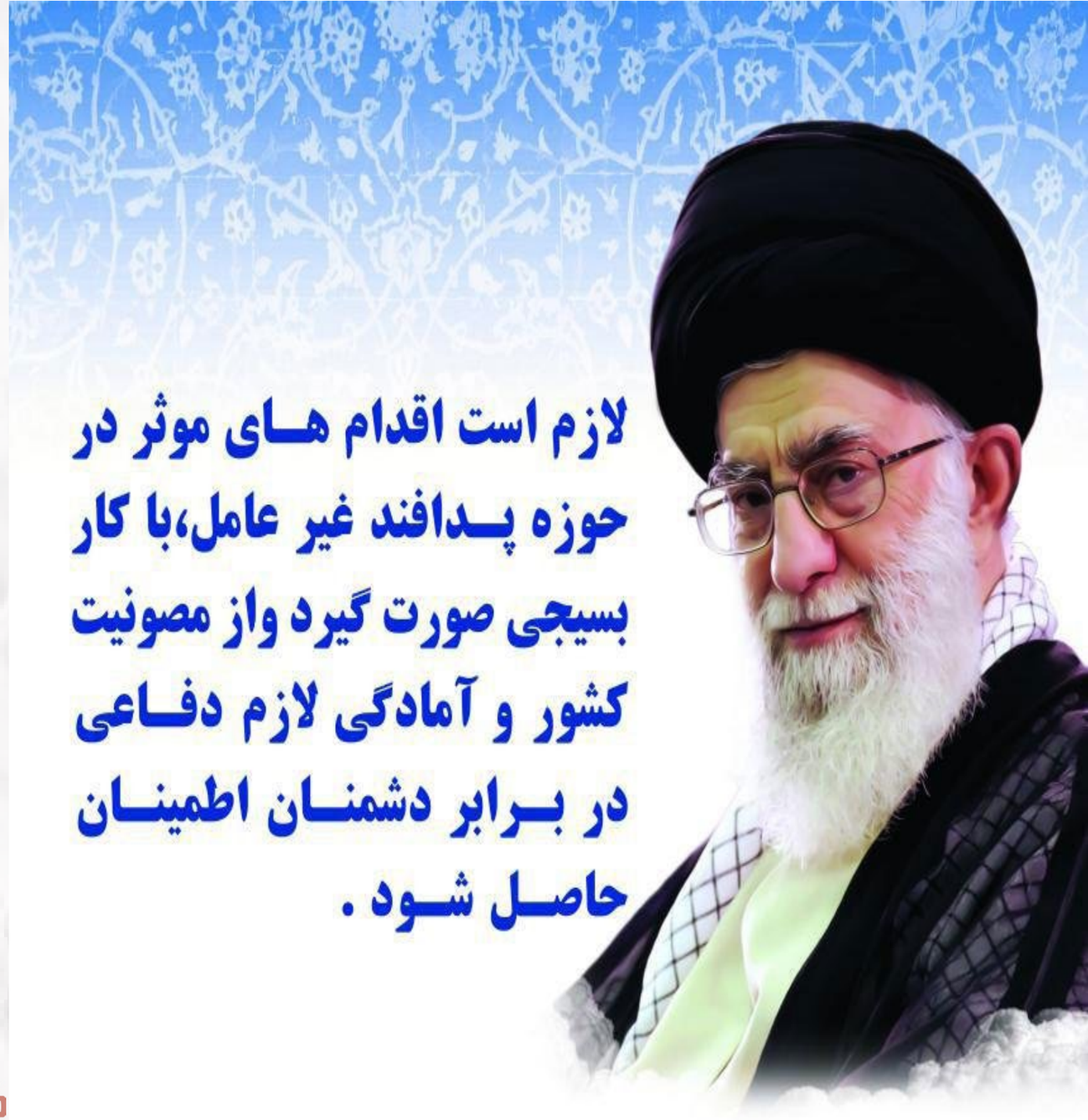
مدیر مسئول:
محمد بیگ

سردبیر:
لیدا رسول اهری

نشانی:
تبریز، میدان شهدا، استانداری آذربایجان شرقی، اداره کل پدافند غیرعامل
تلفن: ۰۴۱-۳۵۲۹۱۳۱۸
دورنگار: ۰۴۱-۳۵۲۹۱۳۵۹

استادان، پژوهشگران و دانشجویان علاقمند، می‌توانند مقاله‌های آموزشی، پژوهشی و ترویجی خود را برای درج در نشریه پدافند غیر عامل به نشانی زیر ارسال کنند.

passivedefence@ostan-as.ir



پدافند غیر عامل ، حصول اطمینان از مصونیت و آمادگی کشور

جلسه کمیته پدافند غیرعامل در منطقه آزاد ارس برگزار شد

- جلسه کمیته پدافند غیرعامل در منطقه آزاد ارس برگزار شد

جلسه کمیته پدافند غیرعامل سازمان منطقه آزاد تجاری صنعتی ارس با حضور معاونت فنی و زیربنائی سازمان پدافند غیرعامل کشور، مدیرکل پدافند غیرعامل استان و فرماندار شهرستان جلفا و اعضای کمیته پدافند غیرعامل سازمان منطقه آزاد تجاری صنعتی ارس تشکیل شد.

طرزی معاونت فنی و زیربنائی سازمان پدافند غیرعامل، وقایع و خرابکاری چندین سال اخیر کشور را ناشی از سهل انگاری و عدم توجه به الزامات پدافند غیرعامل دانسته و به اهمیت موضوعات پدافند غیرعامل و موقعیت پدافند غیرعامل استان پرداخت.

همچنین ایشان بر جدا سازی اینترنت از اینترانت، شناسایی دارایی‌ها، برآورد تهدیدات، احصای تهدیدات و رعایت دقیق الزامات پدافند غیرعامل و تهیه طرح جامع پدافند غیرعامل منطقه آزاد تأکید نمود.

محمد بیگ مدیرکل پدافند غیرعامل استان در این جلسه با اشاره به اهمیت و ضرورت پدافند غیرعامل، بر رعایت الزامات، ملاحظات و اسناد بالادستی و پیش بینی و پیشگیری از موارد مربوطه از منظر پدافند غیرعامل و همچنین استفاده از نیروهای جوان و متعهد، مدیریت میدانی و کارهای تیمی و تخصصی تأکید نمود.

در این جلسه عطاپور فرماندار شهرستان جلفا با اشاره به ویژگی منطقه از جمله همجواری با کشورهای آذربایجان و ارمنستان, بحث آلودگی رودخانه ارس، سد سازی کشور ترکیه در بالادست رودخانه ارس و سایر موارد و مشکلات مربوط، اختصاص اعتبار ویژه از محل اعتبارات پدافند غیرعامل و مدیریت بحران جهت انجام مطالعه و اجرای طرح‌های مربوطه به منظور آمادگی و مقابله برای تهدیدات احتمالی را درخواست نمود.

دکتر کیانی مدیرعامل سازمان منطقه آزاد تجاری صنعتی ارس نیز با اشاره به مشکلات امنیتی منطقه به بیان اهمیت پدافند غیرعامل پرداخته و بر لزوم برنامه ریزی، اولویت بندی و مطالعه طرح جامع پدافند غیرعامل منطقه آزاد ارس با استفاده افراد صاحب نظر و با کمک سایر دستگاه‌های موجود و در راستای دستورالعمل‌ها، قوانین و ابلاغیه‌های پدافند غیرعامل پرداخت.

مدیرکل پدافند غیرعامل استانداری آذربایجان شرقی منصوب شد

استاندار آذربایجان شرقی طی حکمی، محمد بیگ را به عنوان مدیرکل پدافند غیرعامل استانداری منصوب کرد.

در حکم عابدین خرّم خطاب به بیگ آمده است:

نظر به مراتب تعهد و تخصص، جناب‌عالی را به موجب این حکم به عنوان مدیرکل پدافند غیرعامل استانداری آذربایجان شرقی منصوب می‌کنم. امید است با توکل به خداوند متعال با روحیه انقلابی، تعامل سازنده و پیش‌برنده با بخش‌های دولتی و خصوصی، بهره‌مندی از توانمندی‌های اساتید، نخبگان و نیروهای متعهد، دلسوز و کارآمد آن حوزه درخصوص اعمال تدابیر دفاع امنیتی و نهادینه‌سازی دکترین پدافند غیرعامل در استان، در عمل به فرامین مقام معظم رهبری در پیشبرد اهداف نظام مقدس جمهوری اسلامی و سیاست‌های دولتی مقتدر و مردمی موفق و موید باشید.

محمد بیگ متولد ۱۳۶۱ در شبستر و دارای مدرک کارشناسی ارشد علوم کامپیوتر با گرایش هوش مصنوعی است که در رده‌های مختلف اجرایی و مدیریتی ازجمله کارشناسی حوزه‌های پدافند غیرعامل، فناوری اطلاعات و شبکه دولت، فرهنگی و اجتماعی و امور سیاسی و انتخابات در فرمانداری‌های شبستر و مرند و استانداری آذربایجان شرقی و مشاور معاون سیاسی، امنیتی و اجتماعی استاندار مشغول به کار بوده است.

جلسه بررسی کاهش مخاطرات حوادث و سوانح در حوزه پدافند غیرعامل

جلسه توجیهی «بررسی کاهش مخاطرات حوادث و سوانح و رتبه بندی آن در حوزه پدافند غیرعامل» به ریاست مدیرکل پدافند غیرعامل استانداری آذربایجان شرقی تشکیل شد.

محمد بیگ در این جلسه گفت: در حوزه عمل و وظایف بحران و پدافند غیرعامل اشتراکات زیادی وجود دارد همین امر باعث شده سازمان پدافند غیرعامل و وزارت کشور در خصوص ادغام یا تفکیک وظایف آن‌ها تجدید نظر کند.

وی خاطرنشان کرد: ۵۶ مخاطره که امکان وقوع آن‌ها در کشورمان وجود دارد، از طریق سازمان بحران کشور شناسایی شده که جهت تهیه و تدوین برش استانی و شهرستانی به استان‌ها ارجاع شده و دستگاه‌های اجرایی و متولیان استانی نیز بایستی با نظر کارشناسی و دقیق نسبت به تدوین سند و اولویت‌بندی مخاطرات ارجاعی اهتمام بورزند.

حسین‌پور، نماینده مجری طرح در استان نیز با بیان اینکه از بین ۵۶ مخاطره شناسایی شده، ۱۵ مخاطره در مرکز استان پیش بینی شده، تأکید کرد: بر اساس نظرات و پیشنهادات دستگاه‌های اجرایی استانی و شهرستانی، تعداد این مخاطرات قابل افزایش و حتی کاهش یا به نوعی قابل ادغام و تفکیک نیز می‌باشد.

وی ادامه داد: پس از تکمیل و تدوین سند راهبردی برش استانی و شهرستانی در راستای مهار و مقابله با مخاطرات و مدیریت پاسخ به عملیات، قاعدتاً بودجه نیز بر همین اساس تخصیص خواهد یافت. لذا لازم است کلیه دستگاه‌ها باید در جهت تکمیل این سند همکاری حداکثری داشته باشند.

جلوگیری از تبخیر آب

تهیه و تنظیم: حبیب حامدی مارالانی (کارشناس امریه اداره کل پدافند غیرعامل)

مقدمه

اگرچه بیش از ۷۰٪ سطح زمین توسط آب پوشیده است، اما فقط ۱٪ از این میزان آب قابل آشامیدن است. علاوه براین، رشد جمعیت، آلودگی و گرمایش جهانی، تأثیرات شگرفی بر منابع آبی دارند. پدیده تبخیر یکی از فرایندهای کاهش کیفی و کمی آب در دسترس است. میزان تبخیر در نواحی مختلف ایران عبارت است از: سواحل دریای خزر (۱۰۰۰ تا ۱۵۰۰ میلی‌متر)، پهنه مرکزی (۲۰۰۰ تا ۳۰۰۰ میلی‌متر) و ساحل‌های خلیج فارس(۳۰۰۰ تا ۵۰۰۰ میلی‌متر). این داده‌ها اهمیت کاربرد روش‌های مختلف جهت جلوگیری از میزان تبخیر از سطح آب دریاچه‌های سدها را نشان می‌دهد.

تبخیر آب عبارت است از فرآیندی که در آن آب مایع به بخار آب تبدیل می‌شود. مولکول‌های آب در حال حرکت هستند و بعضی از آن‌ها انرژی لازم برای فرار به هوای مجاور به صورت بخار آب را دارند. عوامل مؤثر در تبخیر از سطح مخزن‌ها عبارت است از مساحت سطح آب، دمای هوا، کمبود فشار بخار هوا، سرعت باد، فشار اتمسفر و کیفیت آب.

روش‌های متعددی در سراسر جهان برای ذخیره‌سازی آب از قبیل روش‌های فیزیکی (پوشش‌های شناور)، شیمیایی و بیولوژیکی (گیاهان آبزی و برگ درخت نخل) توسعه داده شده است. تلاش‌های صورت پذیرفته در این مورد از سال ۱۹۶۰ و با استفاده از لایه‌های مولکولی به عنوان مانع غیرقابل نفوذ برای سطح آب آغاز شد. پس از این تاریخ، روش‌های متعددی نیز در راستای کنترل بهتر تلفات ناشی از تبخیر آب‌های سطحی ارائه گردیده است.

پوشش‌های پیوسته شناور

پوشش‌های شناور به طور کلی مانعی غیرقابل نفوذ و شناور بر روی سطح آب در راستای کاهش میزان تبخیر آب ایجاد می‌کند. مصالح پلی استایرن، واکس و فوم برای پوشش‌های پیوسته شناور به کار برده شده است اما پلاستیک پلی اتیلن به عنوان پذیرفته‌ترین و با دوام‌ترین مصالح در این زمینه شناخته شده است. آزمایشات نشان داده است که صفحات پیوسته شناور مانند *E-VapCaps* می‌توانند تا ۹۵٪ از تبخیر در منابع ذخیره‌سازی آب‌های آزاد را کاهش دهند.

پوشش‌های ماژولار شناور

برخلاف پوشش‌های پیوسته شناور، پوشش‌های ماژولار شناور، می‌توانند آزادانه شناور باشند در حالی که تمام سطح آب را پوشش نمی‌دهند. به همین دلیل این پوشش ها امکان انتقال اکسیژن را از طریق فضاهای باز موجود بین خود فراهم می‌آورند.

کلاهک‌های آبزی و توپ‌های سایه انداز نمونه‌هایی از پوشش‌های ماژولار شناور می‌باشند. این نوع از پوشش‌ها، مدور و یا گنبدی شکل بوده و از جنس پلی پروپیلن و پلی اتیلن با چگالی بالا می‌باشند. در این پوشش‌ها یک سوراخ به قطر ۱۰ میلی‌متر تعبیه گردیده تا از این طریق تعادل فشار برقرار شده و هوا از این طریق خارج گردد.

توپ‌های سایه‌انداز از جنس پلاستیک دوست‌دار محیط زیست بوده که می‌توانند در دریاچه‌ها، مخازن جریان و سدها استفاده شوند. نخستین بار از این سیستم در سال ۲۰۱۱ و در لوس آنجلس کالیفرنیا توسط دپارتمان آب و انرژی (*LADWP*) بهره گرفته شد.

این پوشش باعث جلوگیری از تبخیر و نفوذ اشعه *UV* به عنوان عامل ایجاد فرایندهای مخرب می‌شود. طی پژوهشی که در کشور هندوستان در این زمینه صورت پذیرفت، اثر استفاده این توپ‌ها در کاهش میزان تبخیر در آب‌های سطحی بررسی شد. در این پژوهش که از توپ‌های سیاه و ٤ اینچی از جنس پلی اتیلن با چگالی بالا استفاده شد، کاهش ٤٣٪ تا ٤٥٪ میزان تبخیر مشاهده گردید.

پوشش‌های سایه‌ای

پوشش‌های سایه‌ای، سازه‌هایی نصب شده در سطح آب می‌باشند که دارای المان‌های پایه و کابل‌های فلزی هستند. این پوشش اثر باد را کاهش داده و تابش اشعه را مانع می‌شود و از این طریق نرخ تبخیر از سطح آب را تقلیل می‌دهد. با توجه به مقاصد اقتصادی، این نوع از پوشش برای منابع ذخیره آب با مساحت کوچکتر از ۲۰ هکتار استفاده می‌شود.

طی پژوهشی که در اسپانیا و در فصل تابستان انجام پذیرفت، عملکرد پوشش‌های سایه ای در کاهش تبخیر از سطح آب با استفاده از دو پوشش کلاس *A*، یک نمونه بدون پوشش و دیگری با پوششی از جنس دیگر شامل پوشش‌های تک و دو لایه پلی اتیلن با رنگ‌های مختلف و یک لایه آلومینیومی مورد بررسی قرار گرفت. در نتیجه این آزمایش، کاهش ۵۰٪ و ۸۰٪ به ترتیب برای پوشش‌های آلومینیومی و پلی اتیلنی رنگی مشاهده گردید. این پژوهش نشان داد که برخی مؤلفه‌ها از قبیل رنگ، تخلخل و توانایی بهبود تراکم در طول شب در انتخاب نوع پوشش مدنظر قرار می‌گیرند.

پوشش صفحات خورشیدی

استفاده از پوشش صفحات خورشیدی بر روی کانال‌های آب، باعث کاهش چشمگیر میزان تبخیر می‌گردد. به طور

منابع:
۱- پیری؛ مهدی، حسام؛ موسی، دهقانی؛ امیر احمد، مفتاح هلقی؛ مهدی، غزلی؛ علی اکبر، «بررسی تأثیر استفاده از الکل‌های سنگین بر کاهش تبخیر از سطح مخازن آب»، مجله علوم کشاورزی و منابع طبیعی، جلد شانزدهم، ۱۳۸۸.
۲- سپاس خواه؛ علی رضا، «کاهش تبخیر از مخزن آب سدها»، مجله پژوهش‌های راهبردی در علوم کشاورزی و منابع طبیعی، جلد ۳، ۱۳۹۷.
۳- شرایعی؛ مریم، حقایقی اقدم؛ سید ابوالقاسم، «مروری بر روش‌های کاهش تبخیر از سطح آزاد آب و معرفی شیوه‌های مناسب کاربردی و اقتصادی»، نشریه آب و توسعه پایدار، سال هفتم، شماره ۲، ۱۳۹۹.
٤. Waheeb Youssef, Khodzinskaya Anna, «A Review of Evaporation Reduction Methods from Water Surfaces», E3S Web Conferences, ۲۰۱۹.
٥. I.P. Craig, «Loss of storage water due to evaporation – a literature review", NCEA publication, University of Southern Queensland, Australia, ۲۰۰٥.
٦. X. Yao, H. Zhang, C. Lemckert, A. Brook, P. Schouten, «Evaporation Reduction by Suspended and Floating Covers: Overview, Modelling and Efficiency", Technical Report No. ۲۰۱۰, ۲۸.
۷. H. Baldwin, «Assessment of Floating Hard Covers on Large Water Storages», Urban Water Security Research Alliance, technical report No. ۲۰۱۰, ۲۷.
۸. P.Vasantha Kumar, S.V.Naveen Kumar, P.Saravana Kumar, S.Subash, M.Sivaraja ۲۰۱۸.

مثال در سال ۲۰۱۴، یک نیروگاه خورشیدی ۱۰ مگاواتی در هندوستان و با ارزش ۱۸٫۳ میلیارد دلار افتتاح شد. این سیستم حدود ۳٫۶ کیلومتر از طول کانال آبیاری نارمادا در غرب هندوستان را تحت پوشش قرار داده و شامل ۳۳۸۱۶ صفحه خورشیدی می‌باشد.

در نتیجه این پوشش، حدود ۹ میلیون لیتر آب در سال ذخیره گردید. علاوه بر این، خاصیت خنک شوندگی طبیعی نیروگاه‌های خورشیدی نصب شده بر روی کانال آب، باعث افزایش اثرگذاری این پنل‌ها به میزان ۷% نسبت به پنل‌های زمینی می‌شود.

گیاهان آبزی شناور

گیاهان آبزی شناور می‌توانند باعث کاهش میزان تبخیر از سطح آب با جلوگیری از ارتباط بین هوا و لایه مرزی آب شود. برگ درخت نخل از جمله این پوشش‌ها می باشد که در این زمینه نیز طی پژوهشی تأثیر ۵۵% و ۲۶% در کاهش میزان تبخیر آب در حالت پوشش کامل و نیمه پوشیده استخر مشاهده گردید. لازم بذکر است که برخی از گیاهان کیفیت آب را تحت تأثیر قرار می‌دهند و باید قبل از کاربرد، مطالعات لازم در این زمینه صورت پذیرد.

استفاده از الکل‌های سنگین

در برخی از روش‌های شیمیایی از یک لایه تک مولکولی الکل‌های چرب با زنجیره بلند روی سطح آب استفاده می‌شود. مولکول‌های این مواد از یک قطب، آب را به شدت جذب و از طریق قطب دیگر آب را به شدت دفع می‌کنند. وقتی این مولکول‌ها داخل آب قرار می‌گیرند، طوری تغییر جهت می‌دهند که یک قطب آن‌ها داخل آب و قطب دیگر به سمت بالا و خارج از آب قرار می‌گیرد.

در حالت ایده آل می‌توان یک لایه از این مولکول‌ها را روی سطح آب قرار داد و با این لایه تک مولکولی تبخیر از سطح آب را کنترل نمود. ضخامت این فیلم ماده شیمیایی معمولاً از یک نانومتر کمتر است. این لایه نامرئی است و هیچ یک از ناهنجاری‌های فیلم‌های روغن مرئی را ایجاد نمی‌کند. وجود این لایه تک مولکولی روی سطح آب از ایجاد موج‌های کوچک جلوگیری می‌کند. این فیلم آبی توسط قطره‌های باران شکسته شده و پس از نفوذ باران بلافاصله بسته می‌شود.

در روش کنترل شیمیایی، الکل‌های چرب برای اولین بار در اوایل دهه ۱۹۵۰ در استرالیا مورد آزمایش قرار گرفتند. در این روش بیشتر از ستیل الکل‌ها مانند هگزادکانول که یک جامد کریستالی با حالت واکسی و سفید رنگ است و به صورت پولک یا پودر عرضه می‌شود و نیز استریل الکل‌ها مثل اکتادکانول، استفاده می‌شود. وزن مخصوص این مواد از آب کمتر است. میزان مصرف تئوری این الکل‌ها برای کاهش تبخیر، کمتر از ۲۵ گرم بر هکتار می‌باشد ولی در عمل به دلیل اثر باد، جانوران آبی و حشرات، میزان مصرف از این مقدار بیشتر است.

میزان کاهش تبخیر با استفاده از اکتادکانول نسبت به هگزادکانول بیشتر می‌باشد و با ترکیب این الکل‌ها به نسبت مساوی می‌توان کاهش تبخیر بیشتری را مشاهده نمود. نتایج نشان می‌دهد با استفاده از این الکل‌ها و نحوه اجرای صحیح آن، می‌توان ۴۰ تا ۵۵ درصد از میزان تبخیر را کاهش داد.

همچنین با افزایش غلظت از ۲۰ تا ۴۰ گرم بر هکتار میزان کاهش تبخیر نیز بیشتر می‌شود.

معمولاً پولک‌های جامد ستیل الکل‌ها و استریل الکل ها به روش‌های زیر مورد استفاده قرار می‌گیرند:

۱- به صورت محلول با استفاده از یک حلال مناسب مثل تورپنتاین معدنی که برای حل ستیل الکل‌ها مناسب است. کروزین و الکل اتانول از حلال‌های دیگر به شمار می‌روند.

مزایای روش استفاده از محلول: سرعت پخش زیاد، کم بودن مقدار مواد لازم برای تولید یک فیلم آبی و سهولت کاربرد برای استفاده مداوم. مهم‌ترین عیب این روش هزینه زیاد ماده حلال است.

۲- به صورت پودر ریز

۳- به صورت امولسیون یا سوسپانسیون: در این روش پودر ستیل الکل به ۱ تا ۲ گالن آب حاوی کمی صابون یا سورفکتانت‌ها اضافه شده و تا حرارت ۶۷ درجه سانتی‌گراد گرم می‌شود تا به شکل خمیر درآید و سپس این خمیر تا حجم مورد نظر رقیق می‌گردد. معمولاً آب شیر برای این کار مناسب است. برای کنترل تبخیر و نگهداری فیلم ستیل الکل روی سطح آب کاربرد این مواد هر روز صورت می‌گیرد.

۴- استفاده از دانه‌های ریز ستیل الکل: لازم بذکر است با افزایش سرعت باد از ۷ متر بر ثانیه، عملکرد الکل‌ها کم می‌شود، بنابراین استفاده از این روش در مناطقی که متوسط سرعت باد در آن‌ها بیش از این مقدار است تأثیر مثبتی نخواهد داشت.

تزریق حباب هوا به آب

سطح آب در فصل تابستان گرم شده و چگالی آن کم می شود. در زیر این لایه که دارای عمقی به میزان ۳ تا ۴ متر است، آب چگالی بیش‌تری داشته و سرد است. این دولایه از طریقی مرزی از هم جدا می‌شوند که از این طریق، از تداخل این دولایه با هم جلوگیری می‌شود. این حالت موسوم به حالت طبقه‌بندی یا قشربندی است. با تزریق حباب هوا به آب سرد لایه عمیق، پدیده قشرزدایی مصنوعی رخ می‌دهد. در نتیجه این فرآیند و با توجه به یکنواخت شدن اختلاف دمایی نسبت به عمق آب، تبخیر آب کاهش می‌یابد.

کوبرگ و فورد نخستین پژوهشگرانی بودند که استفاده از ستون حباب را برای جلوگیری از تبخیر آب پیشنهاد دادند. آن‌ها اثرات تزریق حباب هوا را بر دما و میزان تبخیر دریاچه ووهلفورد در کالیفرنیا آمریکا در سال ۱۹۶۲ بررسی نمودند.

یک سیستم تزریق حباب هوا به طور مستمر طی سه ماه فرآیند تزریق حباب را انجام می‌داد. میزان دمای آب در جهت مقایسه با مقادیر سه سال گذشته (بدون سیستم تزریق حباب هوا) مشاهده و ثبت گردید. نرخ تبخیر آب نیز با استفاده از روش‌های غیرمستقیم و از طریق دمای اندازه‌گیری شده تخمین زده شد.

نتایج پژوهش نشان داد که در مقایسه با سه سال پیش، در سال ۱۹۶۲ دمای سطح آب پایین بوده و همچنین میزان تبخیر نیز ۱۵% در طول تابستان کاهش یافته و در زمستان ۹% افزایش یافته است. این تفاوت‌ها با استفاده از روش تزریق حباب هوا در سال ۱۹۶۲ بهبود داده شد. در نتیجه این سیستم بیانگر ظرفیت ذخیره آب به میزان ۶% در سال است.

بادشکن

ساختمان بادشکن می‌تواند از ساخت دیوارهای بلند در اطراف منبع تا کاشت درختان در اطراف آن را شامل شود. در صورت امکان، بهتر است منبع آب جایی قرار بگیرد که از عوارض طبیعی مثل تپه‌ها برای کاهش دادن سرعت باد در اطراف آن بهره‌گیری شود. استفاده از درخت به عنوان بادشکن مزایایی به دنبال دارد، از جمله این که می‌توان زمان زیادی از آن استفاده کرد.

البته باید توجه داشت که درختان نباید بسیار نزدیک به منبع آبی کاشته شوند، زیرا ریشه آن‌ها جذب آب بیشتری از مخزن خواهند داشت. درختان مناسب به عنوان بادشکن از نوع درختان مخروطی مثل کاج و سرو، اقاقیا و اکالیپتوس می‌باشند.

لایروبی مخازن

در صورتیکه در مخزن مورد نظر، رسوبات بیش از حد باشد، لایروبی مخزن نیز می‌تواند به کاهش تبخیر کمک کند که البته فواید و الزامات دیگری نظیر جلوگیری از کاهش حجم مخزن، افزایش کیفیت آب و ... دارد. در یک تحقیق بر روی یک نمونه سد مشخص شد که رسوب‌گذاری طی زمان، هندسه این مخزن را به سمت یک مخزن نسبتاً وسیع و کم‌عمق تغییر داده و باعث شده که تبخیر از سطح مخزن در رقوم نرمال آن، حدود ۳۰ درصد نسبت به سال شروع بهره‌برداری افزایش یابد.

روش‌های مدیریتی

می‌توان با اعمال روش‌های مدیریتی مختلف، میزان تبخیر کل را کاهش داد. آب را می‌توان بین مخازن پمپ نمود تا سطح مقطع در واحد حجم آب ذخیره شده، حداقل گردد. چرخش آب همچنین می‌تواند باعث کاهش دمای سطح آب و کاهش نرخ تبخیر شود.

روش‌های طراحی یا ساختمانی

به طور کلی هنگام احداث سد باید توجه داشت که در صورت امکان، محل سد طوری انتخاب شود تا نسبت سطح مخزن به حجم آن، حداقل شود. همچنین برای جلوگیری از گسترش سطح آزاد آب دریاچه، دیوارچینی ساحل دریاچه در نواحی کم‌عمق و کم‌شیب صورت گیرد، به این منظور می‌توان ساختار سلولی ایجاد نمود که در آن مخازن بزرگ به سلول‌های کوچک تقسیم می شوند تا بتوان سرعت و تأثیر باد را کاهش داده با انتقال آب میان سلول‌ها و استفاده از بادشکن اطراف مخزن، عمق آب را حداکثر نمود.

برای حداکثر نگه داشتن عمق آب، باید به وسیله پمپ کردن آب از سلول‌های نیمه خالی به همدیگر، سطح موجود برای تبخیر را به حداقل رسانید. در کشور ژاپن با استفاده از سیستم آبگیری تلسکوپی که در سدهای سامه اورا و تومی ساتو به کار برده‌اند، امکان آبگیری از ترازهای مختلف مخزن را فراهم نموده و در کنترل پدیدهٔ لایه‌بندی دمایی آب مخزن و در نظر گرفتن ملاحظات کیفی آب، موفق عمل نموده‌اند.

آسیب‌پذیری

آسیب‌پذیری در محصولات VMware

VMware تعداد ۱۰ نقص امنیتی را در محصولات خود برطرف نموده است. این شرکت همچنین در خصوص وصله آسیب‌پذیری بحرانی دور زدن فرآیند احراز هویت در برخی از محصولات خود که کاربران *local domain* را تحت تأثیر قرار می‌دهد و مهاجم احراز هویت نشده را قادر می‌سازد تا امتیازات ادمین را به دست آورد، به مدیران هشدار داد.

جزئیات آسیب‌پذیری

CVE-۲۰۲۲-۳۱۶۵۶: این آسیب‌پذیری با شدت بحرانی که در محصولات *VMware Workspace ONE Access* و *Identity* Manager و *vRealize Automation* شرکت *VMware* وجود دارد، یک نقص دور زدن فرآیند احراز هویت است که کاربران *local domain* را تحت تأثیر قرار می‌دهد. یک مهاجم با دسترسیِ شبکه به رابط کاربری ممکن است بتواند بدون نیاز به احراز هویت دسترسی ادمین را به دست آورد.

CVE-۲۰۲۲-۳۱۶۵۸: این آسیب‌پذیری با شدت بالا که در محصولات *VMware Workspace ONE Access* و *Identity Manager* و *vRealize Automation* شرکت *VMware* وجود دارد، یک نقص اجرای کد از راه دورِ تزریق *JDBC* است که به مهاجم با دسترسی ادمین در شبکه اجازه می‌دهد کد دلخواه خود را از راه دور اجرا نماید.

CVE-۲۰۲۲-۳۱۶۵۹: این آسیب‌پذیری با شدت بالا که در محصولات *VMware Workspace ONE Access* و *Identity Manager* شرکت *VMware* وجود دارد، یک نقص اجرای کد از راه دورِ تزریق *SQL* است که به مهاجم با دسترسی ادمین در شبکه اجازه می‌دهد کد دلخواه خود را از راه دور اجرا نماید.

CVE-۲۰۲۲-۳۱۶۶۰ و *CVE*-۲۰۲۲-۳۱۶۶۱: این دو آسیب‌پذیری با شدت بالا که در محصولات *VMware Workspace ONE Access*، *Identity Manager* و *vRealize Automation* شرکت *VMware* وجود دارند، نقص‌های ارتقاء سطح دسترسی هستند که به مهاجم با دسترسی محلی اجازه می‌دهند سطح دسترسی خود را به *'root'* ارتقاء دهد.

CVE-۲۰۲۲-۳۱۶۶۴: این آسیب‌پذیری با شدت بالا که در محصولات *VMware Workspace ONE Access* و *Identity Manager* و *vRealize Automation* شرکت *VMware* وجود دارد، یک نقص ارتقاء سطح دسترسی است که به مهاجم با دسترسی محلی اجازه می‌دهد سطح دسترسی خود را به *'root'* ارتقاء دهد.

CVE-۲۰۲۲-۳۱۶۶۵: این آسیب‌پذیری با شدت بالا که در محصولات *VMware Workspace ONE Access* و *Identity Manager* و *vRealize Automation* شرکت *VMware* وجود دارد، یک نقص اجرای کد از راه دورِ تزریق *JDBC* است که به مهاجم با دسترسی ادمین در شبکه اجازه می‌دهد کد دلخواه خود را از راه دور اجرا نماید.

CVE-۲۰۲۲-۳۱۶۵۷: این آسیب‌پذیری با شدت متوسط که در محصولات *VMware Workspace ONE Access* و *Identity Manager* شرکت *VMware* وجود دارد، یک نقص تزریق *URL* است که به مهاجم با دسترسیِ شبکه اجازه می‌دهد یک کاربر احراز هویت شده را به دامنه دلخواه هدایت کند.

CVE-۲۰۲۲-۳۱۶۶۲: این آسیب‌پذیری با شدت متوسط که در محصولات *VMware Workspace ONE Access*، *Identity Manager*، *Connectors* و *vRealize Automation* شرکت *VMware* وجود دارد، یک نقص *path traversal* است که به یک مهاجم با دسترسیِ شبکه اجازه می‌دهد به فایل‌های دلخواه دسترسی پیدا کند.

CVE-۲۰۲۲-۳۱۶۶۳: این آسیب‌پذیری با شدت متوسط که در محصولات *VMware Workspace ONE Access*، *Identity Manager* و *vRealize Automation* شرکت *VMware* وجود دارد، یک نقص *reflected cross-site scripting (XSS)* است که به دلیل پاک‌سازی نامناسب ورودی‌های کاربر ایجاد می‌شود و به مهاجم اجازه می‌دهد با برخی از تعاملات کاربر بتواند کد جاوااسکریپت را در پنجرهِ کاربرِ موردِ هدف تزریق کند.

مهمترین به‌روزرسانی‌های ماه جاری شرکت‌های تولید کننده سخت افزار و نرم افزار

شرکت مایکروسافت، با انتشار جدیدترین مجموعه اصلاحیه‌های امنیتی ماهانه خود بیش از ۱۲۰ آسیب‌پذیری را در *Windows* و محصولات مختلف این شرکت ترمیم کرد. درجه اهمیت ۱۷ مورد از آسیب‌پذیری‌های ترمیم شده این ماه «حیاتی» و اکثر موارد دیگر «مهم» اعلام شده است. این مجموعه اصلاحیه‌ها، انواع مختلفی از آسیب‌پذیری‌ها را در محصولات مایکروسافت ترمیم می‌کنند، همچون:

«ترفیع اختیارات» (*Elevation of Privilege*)

«اجرای کد از راه دور» (*Remote Code Execution*)

«افشای اطلاعات» (*Information Disclosure*)

«ازکارانداختن سرویس» (*Denial of Service – DoS*)

«عبور از سد امکانات امنیتی» (*Security Feature Bypass*)

«جعل» (*Spoofing*)

دو مورد از آسیب‌پذیری‌های ترمیم شده این ماه (شناسه‌های *CVE*-۲۰۲۲-۳۴۷۱۳ و *CVE*-۲۰۲۲-۳۰۱۳۴)، از نوع «روز-صفر» هستند که از یک مورد آن به طور گسترده در حملات، سوءاستفاده شده است.

آسیب‌پذیری *CVE*-۲۰۲۲-۳۴۷۱۳ دارای درجه اهمیت «مهم» بوده و از نوع «اجرای کد از راه دور» است و به طور گسترده در حملات استفاده شده است.

این ضعف امنیتی بر روی *Microsoft Windows Support Diagnostic Tool* - به اختصار *MSDT* تأثیر می‌گذارد و به *DogWalk* معروف شده است. پس از کشف اثر سوء ضعف مذکور بر روی *MSDT*، محققان امنیتی بار دیگر بر وصله آسیب‌پذیری *DogWalk* تأکید کردند.

دیگر آسیب‌پذیری روز صفر ترمیم شده در این ماه، *CVE*-۲۰۲۲-۳۰۱۳۴ با درجه اهمیت «مهم» و از نوع «افشای اطلاعات» است و به مهاجم اجازه می‌دهد پیام‌های ایمیل را به‌صورت هدفمند بخواند.

ضعف‌های امنیتی با شناسه‌های *CVE*-۲۰۲۲-۲۱۹۸۰، *CVE*-۲۰۲۲-۲۴۵۱۶ و *CVE*-۲۰۲۲-۲۴۴۷۷ همگی از نوع «ترفیع اختیارات» بوده و *Microsoft Exchange Server* از آن‌ها تأثیر می‌پذیرد. شرکت مایکروسافت، احتمال بهره‌جویی از هر سه این آسیب‌پذیری‌ها را «زیاد» اعلام کرده است. هر سه ضعف‌ها برای سوءاستفاده، به احراز هویت و تعامل کاربر نیاز دارند. مهاجم احتمالاً باید از طریق یک حمله «فیشینگ» و دستکاری سرور *Exchange* آسیب‌پذیر، هدف موردنظر خود را ترغیب کند.

آسیب‌پذیری با شناسه *CVE*-۲۰۲۲-۳۴۶۹۱ از نوع «ترفیع اختیارات» است و بر روی *Active Directory Domain Services* تأثیر می‌گذارد. این آسیب‌پذیری می‌تواند توسط یک مهاجم احراز هویت شده به‌منظور دست‌کاری ویژگی‌های حساب‌ها (*Attributes of Accounts*) و احتمالاً دریافت گواهی‌نامه *Active Directory Certificate Services* مورد سوءاستفاده قرار گیرد. گواهی‌نامه مذکور به مهاجم اجازه می‌دهد تا امتیازات خود را افزایش دهد. لازم به ذکر است که سوءاستفاده از این ضعف امنیتی تنها زمانی امکان‌پذیر است که *Active Directory Certificate Service* در *Domain* اجرا شود.

شرکت گوگل کروم یک بروزرسانی امنیتی جدید برای کاربران ویندوز، لینوکس و مک جهت رفع چندین آسیب‌پذیری و همچنین رفع یک آسیب‌پذیری روز صفر با شدت بالا منتشر کرد. کروم ۱۰۴ با رفع ۱۱ آسیب‌پذیری امنیتی از جمله یک آسیب‌پذیری با شدت بحرانی و ۶ آسیب‌پذیری با شدت بالا که توسط تیم *Google Project Zero* و محققان امنیتی دیگر گزارش شده‌اند، منتشر شد. آسیب‌پذیری بحرانی با شناسه «*CVE*-۲۰۲۲-۲۸۵۲»، به مهاجمان اجازه می‌دهد از راه دور کنترل سیستم را بدست بگیرند. ۵ آسیب‌پذیری روز صفر شناسایی شده است که آخرین آسیب‌پذیری با شناسه «*CVE*-۲۰۲۲-۲۸۵۶» و شدت بالا گزارش شده است. ٤ آسیب‌پذیری دیگر عبارتند از:

CVE-۲۰۲۲-۲۲۹٤، *CVE*-۲۰۲۲-۱۳٦٤

CVE-۲۰۲۲-۱۰۹٦، *CVE*-۲۰۲۲-۰٦۰۹

مرورگر گوگل کروم برای ویندوز، لینوکس و مک تحت تأثیر این آسیب‌پذیری‌ها قرار دارند. طبق گزارش گوگل، نسخه‌های وصله شده ۱۰٤,۰,۵۱۱۲,۱۰۱ برای مک و ۱۰٤,۰,۵۱۱۲,۱۰۲ یا ۱۰٤,۰,۵۱۱۲,۱۰۱ برای ویندوز منتشر شده است. جهت بروزرسانی کروم مراحل زیر را دنبال کنید: به بخش Settings بروید. سپس بر روی گزینه *Help* کلیک کنید. پس از آن باید گزینه *About Google Chrome* را انتخاب کنید. اکنون مرورگر به طور خودکار بروزرسانی جدید را بررسی کرده و آن را نصب می‌کند.

آسیب‌پذیری

آسیب‌پذیری افزایش سطح دسترسی در Secure Web Appliance سیسکو

یک آسیب‌پذیری در رابط مدیریت وب *AsyncOS* سیسکو برای *Secure Web Appliance* که قبلاً به نام *Web Security Appliance (WSA)* شناخته می‌شد، کشف شده است که به یک مهاجم احراز هویت شده اجازه می‌دهد از راه دور دستور دلخواه خود را تزریق کند و امتیازات خود را به امتیازات کاربر *root* افزایش دهد.

جزئیات آسیب‌پذیری

آسیب‌پذیری مذکور با شناسه «*CVE-۲۰۲۲-۲۰۸۷۱*» و شدت بالا گزارش شده است. این آسیب‌پذیری به دلیل اعتبارسنجی ناکافی ورودی ارائه شده توسط کاربر برای این رابط وب اتفاق می‌افتد. مهاجم می‌تواند با احراز هویت از طریق سیستم و ارسال یک بسته *HTTP* جعلی به دستگاه آسیب‌دیده، از این آسیب‌پذیری سوءاستفاده کند. یک بهره‌برداری موفق مهاجم را قادر می‌سازد تا دستورات دلخواه خود را بر روی سیستم عامل اصلی اجرا کند و امتیازات خود را در حد کاربر *root* افزایش دهد. برای بهره‌برداری موفق از این آسیب‌پذیری، مهاجم حداقل به امتیاز *read-only* نیاز دارد.

محصولات تحت تأثیر

این آسیب‌پذیری *AsyncOS* را برای *Secure Web Appliance*، هم در دستگاه‌های مجازی و هم سخت‌افزاری تحت تأثیر قرار می‌دهد.

به تأیید سیسکو، محصولات زیر آسیب‌پذیر نیستند:

- *Email Security Appliance (ESA)* هم در دستگاه‌های مجازی و هم سخت‌افزاری
- *Secure Email and Web Manager* هم در دستگاه‌های مجازی و هم سخت‌افزاری

توصیه‌های امنیتی

به کاربران توصیه می‌شود هر چه سریعتر نرم‌افزار خود را به آخرین نسخه وصله شده، مطابق جدول زیر ارتقاء دهند.

در بیشتر موارد، این نرم‌افزار را می‌توان از طریق شبکه با استفاده از گزینه‌های *System Upgrade* در رابط وب *Secure Web Appliance* ارتقاء داد. جهت ارتقاء دستگاه با کمک رابط وب، مراحل زیر را انجام دهید:

System Administration > System Upgrade را انتخاب کنید.

روی گزینه‌های *Upgrade* کلیک کنید.

Download و *Install* را انتخاب کنید.

نسخه مورد نظر خود را انتخاب کنید.

در قسمت *Upgrade Preparation*، گزینه‌های مناسب را انتخاب کنید.

روی *Proceed* کلیک کنید تا عملیات ارتقاء آغاز شود.

پس از پایان کار دستگاه مجددا راه‌اندازی می‌شود.

آسیب‌پذیری در python-flask-restful-api

مخزن *akashtalole/python-flask-restful-api* در *GitHub* تا نسخه ۲۰۱۹-۰۹-۱۶ دارای آسیب‌پذیری بحرانی است. این آسیب‌پذیری در تابع *send_file* کتابخانه *flask* یافت می‌شود.

چنانچه فراخوانی این تابع در ماژول *app/api/exports./py* با ورودی نامناسب (دنباله‌ای از «*dot-dot-slash* (../)» یا مسیرهای کامل فایل‌ها) انجام شود، می‌تواند باعث حمله پیمایش مسیر شده و دسترسی به فایل‌ها و دایرکتوری‌های اختیاری را که خارج از پوشه ریشه وب قرار دارند، میسر سازد.فراخوانی *os.path.join* برای استفاده با ورودی نامطمئن، امن نیست. هنگامیکه *os.path.join* با استفاده از یک «مسیر کامل» فراخوانی می‌شود، تمام پارامترهای قبلی را نادیده گرفته و شروع به کار با مسیر کامل جدید می‌کند.

برای رفع این آسیب‌پذیری باید از اعمال ورودی نامطمئن به تابع آسیب‌پذیر *send_file* جلوگیری کرد و در صورتیکه مطابق با منطق برنامه، این کار ضرورت داشته باشد، می‌توان از *werkzeug.utils.safe_join* برای استفاده از مسیرهای نامطمئن بهره برد یا فراخوانی‌های *flask.send_file* را با *flask.send_from_directory* جایگزین نمود.

گسترش بدافزار سرقت اطلاعات Amadey به کمک SmokeLoader

نوعی بدافزار سرقت اطلاعات به نام *Amadey* با استفاده از *Backdoor* دیگری به نام *SmokeLoader* در حال گسترش است و چنانچه کاربران بدافزار *SmokeLoader* را به‌عنوان یک کرک نرم‌افزاری نصب کنند، راه را برای استقرار بدافزار *Amadey* هموار می‌کنند. این بدافزار به قابلیت‌هایی مثل استخراج *Credential*های سیستم، گرفتن عکس از صفحه نمایش، ابرداده‌های سیستم، اطلاعات درباره آنتی‌ویروس‌های سیستم و نصب بدافزارهای اضافی روی دستگاه آلوده مجهز شده است.

ترووجان *SmokeLoader* بیشتر با فایل‌های مایکروسافت آفیس، به دستگاه‌های قربانیان نفوذ می‌کند. مهاجمان از مهندسی اجتماعی برای فریب قربانیان احتمالی برای دانلود فایل پیوست و فعال کردن ماکروها استفاده می‌کنند، هنگامیکه کاربر فایل مخرب را دانلود و اجرا کند، بدافزار نیز اجرا می‌شود. بدافزار *SmokeLoader* سعی می‌کند ماهیت مخرب خود را پنهان کند. این کار با پنهان کردن ارتباط سرور *C&C* با ارتباط به وب‌سایت‌هایی مانند *Microsoft.com* و *Adobe.com* انجام می‌شود. علیرغم دریافت پاسخ از وب‌سایت‌های مانند *Microsoft.com* و *Adobe.com* با کد وضعیت ۴۰۴، این درخواست‌ها هم چنان از سمت بدافزار انجام می‌شود.

در بدافزار *SmokeLoader* از تکنیک *PPID spoofing* برای مخفی کردن پردازش خود از دید آنتی‌ویروس‌ها استفاده می‌شود. هدف این بدافزار پردازش برنامه‌هایی مثل *explorer.exe* است که معمولاً در بیشتر دستگاه‌ها در حال اجرا هستند و بعد از تزریق در پردازش جاری مرحله اجرای درخواست‌های مخرب شروع می‌شود. بعد از استقرار، *SmokeLoader* یک *Registry RunKey* را برای ماندگاری در دستگاه قربانی اضافه می‌کند و همچنین یک اسکریپت را در پوشه *Startup* اضافه می‌کند تا *payload* را مستقر کند. بااین‌حال، هدف اصلی این بدافزار استقرار افزونه‌های اضافی و تروجان‌های دسترسی از راه دور، مانند *Remcos RAT* و *RedLine Stealer* است که عامل تهدید را قادر می‌سازد مجموعه‌ای از فعالیت‌های پس از بهره‌برداری را انجام دهد. برای جلوگیری از آلوده شدن به این بدافزار توصیه می‌شود دستگاه‌های خود را به آخرین نسخه‌های سیستم‌عامل و مرورگر وب ارتقا دهند و نرم‌افزارهای کرک شده را به هیچ وجه نصب نکنند.

سوءاستفاده از Windows Defender، تکنیک جدید باج‌افزار LockBit

گردانندگان باج‌افزار *LockBit ۳,۰* از خط فرمان *Windows Defender* و یک سری روال‌های ضد شناسایی و ضد تحلیل برای دور زدن محصولات امنیتی استفاده می‌کنند. *LockBit* از ابزار معتبر خط فرمان *VMware*، به نام *VMwareXferlogs.exe*، برای بارگذاری و تزریق *Cobalt Strike* استفاده می‌کند.

مهاجمان از خط فرمان *Windows Defender* به نام *Windows Defender MpCmdRun.exe* برای رمزگشایی و دانلود کدهای مخرب *Cobalt Strike* سوءاستفاده می‌کنند. در این حملات، نفوذ اولیه به هدف مورد نظر از طریق آسیب‌پذیری *Log4j* در سرور *VMWare Horizon* وصله نشده صورت می‌گیرد.

مهاجمان مؤلفه *Blast Secure Gateway* برنامه را با نصب یک پوسته وب و از طریق فرمان‌های *PowerShell* تغییر دادند. پس از نفوذ اولیه، مهاجمان با استفاده از فرمان‌هایی تلاش می‌کنند که چندین ابزار از جمله *Meterpreter* و *PowerShell Empire* را به کار گرفته و روش جدیدی برای بارگذاری و تزریق *Cobalt Strike* اجرا کنند. در این سری از حملات، به طور خاص، هنگام اجرای *Cobalt Strike*، از ابزار معتبر جدیدی برای بارگذاری یک *DLL* مخرب استفاده می‌شود که کد مخرب را رمزگشایی می‌کند. مهاجمان *DLL* مخرب، کد بدافزاری و ابزار معتبر را با بکارگیری ابزار معتبر خط فرمان *Windows Defender* به نام *MpCmdRun.exe* از سرور کنترل و فرماندهی خود دانلود می‌کنند. همچنین *DLL* مخرب همانند تکنیک‌های به کارگرفته شده پیشین با حذف *userland hook EDR/EPP*، از ابزارهای تشخیصی فرار و ردیابی رویدادها را برای *Windows* و رابط پویش ضد بدافزاری دشوار می‌سازد. استفاده از ابزارها و توابع عادی و سالم سیستم‌عامل و دیگر نرم‌افزارهای کاربردی توسط مهاجمان سایبری برای اهداف خرابکارانه خود بر روی سیستم قربانی، یکی از روش‌هایی است که مهاجمان برای مخفی ماندن از دید سیستم‌های امنیتی و ضدویروس‌های قدیمی و شناسایی نشدن بکار می‌گیرند. به این روش «کسب روزی از زمین» گفته می‌شود.

معرفی کتاب
حوزه پدافند سایبری

کتاب دانستنی‌های سایبری: جلد اول- شبکه های اجتماعی نوشته علی محمد رجبی، مهرداد جعفری بجد و حامد محمدی سپاسی، دربردارنده هشدارهای پیشگیرانه سایبری است که شما را با شیوه‌های مجرمانه در فضای اینترنت و راهکارهای پیشگیری از آن‌ها به خصوص در شبکه‌های اجتماعی آشنا می‌کند. زندگی در فضای مجازی پر سرعت و پر هیاهو نیازمند برخورداری از مهارت و آگاهی‌های زیادی است. این آگاهی‌ها به خصوص به ما کمک می‌کند تا گرفتار مجرمانی که در کمین سرمایه‌ها و داده‌های ما هستند نشویم. کتاب حاضر که اولین جلد از مجموعه محتوای پیشگیرانه در حوزه فضای مجازی است به همت مرکز تشخیص و پیشگیری از جرایم سایبری پلیس فتا ناجا تهیه شده و مطالب آن متناسب با موضوع در قالب عکس‌نوشته و توضیحات تکمیلی جمع آوری شده است و این امر به شما کمک می‌کند تا بتوانید خیلی سریع و در قالب متن‌های کوتاه با راهکار پیشگیری از آن، آشنا شوید.

کلاهبرداری تلفنی از کارمندان: کلاهبرداران سایبری با برخی از کارمندان سازمان‌ها تماس گرفته و خود را یکی از مسئولین مالی آن سازمان معرفی می‌کنند و در ادامه از کارمندان در خواست می‌کنند برخی اطلاعات مالی خود را در اختیار آن‌ها قرار دهند. در این شگرد مجرم سعی می‌کند، کارمندان را به بهانه‌های مختلف نظیر دریافت پاداش و یا واریزی اشتباه به پای عابر بانک برده و از این طریق حساب آن‌ها را خالی کند.

کلاهبرداری از کارمند جوان به بهانه خرید لوازم خانگی: احدی از شهروندان به پلیس فتا مراجعه و عنوان داشت فردی ناشناس با وی بصورت تلفنی تماس گرفته و خود را یکی از کارمندان بخش رفاهی اداره‌ای که شاکی در آن فعالیت می‌کند، معرفی نموده که از تهران با وی تماس گرفته و به شاکی اعلام میدارد تعداد محدودی لوازم خانگی تأمین شده که با تخفیف می‌توانید آن‌ها را خریداری کنید فقط حتماً تا یک ساعت آینده باید مبلغ پیش پرداخت آن‌ها را واریز کنید، شاکی نیز بدون بررسی از صحت موضوع اقدام به واریز یک میلیون تومان به حساب اعلامی نموده و پس از آن دیگر شماره تلفن تماس گیرنده پاسخگوی شاکی نبوده و از لوازم خانگی نیز خبری نمی‌شود.

طرح‌های کسر خدمت سربازی

به اطلاع می‌رساند که سازمان پدافند غیرعامل کشور (مرکز مطالعات پدافند غیرعامل کشور و مرکز مطالعات فنی و مهندسی پایداری ملی کشور) برای دانش‌آموختگان و فارغ‌التحصیلان مقاطع کارشناسی ارشد و دکتری طرح‌هایی برای کسر خدمت سربازی و نخبگی (جایگزین خدمت سربازی) در نظر گرفته است. علاقمندان می‌توانند علاوه بر مراجعه به وب‌سایت‌های مربوطه با مراجعه به اداره کل پدافند غیرعامل استانداری آذربایجان شرقی از روند ثبت‌نام مطلع شوند.

وب سایت مرکز مطالعات فنی و مهندسی پایداری ملی کشور: http://www.mafpa.ir
وب سایت مرکز مطالعات پدافند غیرعامل کشور: http://www.pdrc.ir

سایت های مرتبط با پدافند غیرعامل

وب سایت پایداری ملی
http://www.paydarymelli.ir

مرکز مطالعات پدافند غیرعامل
http://www.pdrc.ir

استانداری آذربایجان شرقی – پدافند غیرعامل
http://www.ostan-as.gov.ir/Page/۴۲/

پلیس فتا
http://www.cyberpolice.ir

مرکز مطالعات فنی و مهندسی پایداری ملی
http://www.mafpa.ir

مرکز مدیریت راهبردی افتای ریاست جمهوری
http://www.afta.gov.ir