کارگاه آموزشی

باج‌افزارها و روش‌های پیشگیری از اخاذی دیجیتال

دکتر مهران گرمه‌ء - مهندس سارا رحیمی دوین - مهندس میلاد حضرتی

مرکز تخصصی آپا دانشگاه بجنورد

چکیده: حملات باج‌افزاری در سال‌های اخیر سبب‌ساز نگرانی‌های عمده‌ای در فضای سایبری جهانی و ملی بوده‌اند. گذشته از پیش‌زمینه‌ها و امکانات مورد نیاز، محرک اصلی این حملات، منافع اقتصادی سهل‌الوصول ناشی از این حملات است. در این ارایه به بررسی پیش‌نیازها، انگیزه‌ها، نیرنگ‌ها و ترفندهای ورود و جزییات و مراحل انجام یک حمله باج‌افزاری پرداخته می‌شود. همچنین برخی از انواع متداول از حملات باج‌افزاری در این ارایه به صورت عملی بررسی می‌شوند. در انتها با بررسی برخی از نمونه‌های فرآیندهای امدادی به رخدادهای باج‌افزاری، روند کلی امداد در این حملات معرفی می‌شود.

سرفصل کارگاه:

- مقدمه‌ای بر امنیت اطلاعات
- حملات متداول امروز در بستر اینترنت
- دلیل توجه ویژه به حملات باج‌افزاری
- پیش‌نیازهای موفقیت یک حمله باج‌افزاری
- کاربرد رمزنگاری‌های متقارن و نامتقارن
- راه‌های نفوذ باج‌افزارها
- راه‌های باج‌خواهی و دریافت ایمن پول
- راه‌های امن برقراری ارتباط به صورت ناشناس
- استفاده غیر اصولی از آدرس IP معتبر و مشکلات ناشی از سرویس دسترسی از راه دور
- Ransomware as a Service
- گروه‌بندی حملات باج‌افزاری
- معرفی نمونه‌هایی از باج‌افزاهای فارسی‌زبان و غیرفارسی‌زبان و شیوه‌های مختلف عملکرد آن‌ها و برخورد با مهاجمین فارسی زبان
- مهندسی معکوس باج‌افزارهای WannaSmile و ZCrypt
- اجرای نمونه‌هایی از باج‌افزار
- پیشگیری
- پشتیبان‌گیری و به‌روزرسانی

- طرح بازگشت از فاجعه (Disaster Discovery Plan)
- امداد، اقدامات تامینی، اقدامات فنی اولیه
- تشخیص روش ورود
- پیشگیری از رخداد مجدد
- ارزیابی خسارت
- بررسی امکان بازگشایی اطلاعات

مدت زمان کارگاه: ۴ ساعت

زمان برگزاری: پنج‌شنبه ۱۷ اسفند ۱۳۹۶ – ساعت ۱۲-۸