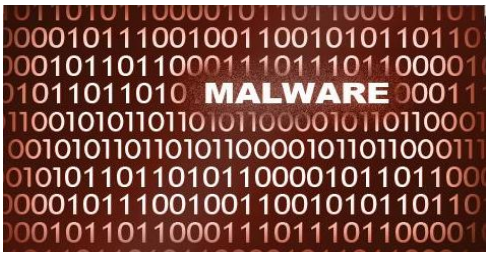

Zararlı Yazılım Analiz Eğitimi

Genel Bakış
Önceleri hobi amaçlı geliştirilen ve tarihi 80li yıllara dayanan zararlı yazılımlar, bugün hedef ve strateji değiştirerek kurumların en büyük tehditi olmuştur. Siber suç örgütleri gerek son kullanıcıları , gerek kurumları hedef alan saldırılarında zararlı yazılımlardan yararlanmaktadır.

Dört günlük bu eğitimin amacı zararlı yazılım analiz tekniklerini teorik ve pratik olarak katılımcılara anlatmaktır. Katılımcılar eğitim sonunda çeşitli tersine mühendislik yöntemleri ile zararlı yazılım analiz methodlarını öğrenerek günlük hayatta karşılaştıkları şüpheli dosyaları analiz edebilecek seviyeye gelecektir.

Eğitimin Katkısı
Katılımcılar eğitimin sonunda, günlük hayatta karşılaştıkları şüpheli dosyaları nasıl analiz edebilecekleri ve iz sürebileceklerini öğrenmiş olacaklardır.

Hedef Kitle
Bilgi Güvenliği Çalışanları, Network / Sistem Uzmanları, Yazılım Geliştiriciler, Kamu Güvenliği Çalışanları

Eğitim İçeriği

***Malware - Giriş**
- Malware Atakları
- Etkisi

***Malware İsimlendirme Standardı**
-Platform
-Programlama Dilleri
-Dosya Formatları ve Uzantıları

***Malware Kategorizasyonu**
- Exploit, Virus, RAT, Backdoor, Rootkit, Worm

***Malware Platformları**
- Windows, Linux, Android, iOS, MacOS, WinCE

***Atak Vektörleri**
- Exploitler, File Infectors, USB, Bluetooth, Emails, Web

***Malware Kod Türleri**
- Polymorphism ve Metamorphism

***Malware Analiz Ortamı (Lab Setup)**
- Virtual OS, Tools (IDA, Debuggers, PE Editors, Sysinternals Tools, HEX Editor and Network Sniffers etc.)

***Tersine Mühendislik Teknikleri**
- Static Analiz
- Dinamik Analiz

*** x86 Mimarisi ve Assembly**
- CPU Mimarisi, Registers, Hafıza Yönetimi
- Assembly Instructions
- Dosya Formatları (PE, ELF, DEX)
- Win32 API

*** Malware Enfeksiyon Kapısı : Exploitler ve Geliştirme Temelleri**
- Hafıza Tabanlı Güvenlik Açıkları (Memory Corruptions)
- Exploit Geliştirme Teknikleri
- Stack Buffer Overflow, Heap Spray, Shellcode

***Malware Analiz Örnekleri**
* Statik Analiz Örnekleri
* Dinamik Analiz Örnekleri
* Otomatize Analiz (Anubis, Scanners, Sandbox etc.)
* Manual and Otomatize Unpacking
* Client-side Malware Analiz (Browser , Office ve PDF Exploit/Malware Analizi)

SignalSEC Information Security Consulting, Software and Technology Services Ltd.
SignalSEC Ltd. is a research company that provides information security services.The main mission of SignalSEC is providing effective vulnerability intelligence services to the customers.

SignalSEC Research team is an active team in international infosec community. Researchers of SignalSEC speak at international security conferences, discover vulnerabilities and publish security advisories.

Address:
SIGNALSEC Bilgi Guvenlik Dan. Yazılım ve Teknoloji Hiz. Tic. Ltd. Sti.
1145/7 Sok. No: 2 D: 210 Uzbek Ishani
35110 Konak, Izmir / TURKEY
Phone: +90 232 433 0DAY
Fax: +90 232 469 85 62
Email: info@signalsec.com
Web: www.signalsec.com