Microsoft

Purple Team: Probando nuestras propias defensas.

Julio Ureña
Technical Specialist Security & Compliance

net user juliourena

- aka PlainText
- Christian / Husban / Father / Friend / Gamer
- Microsoft Technical Specialist Security & Compliance
- Certifications: OSCP, OSEP, CRTO, PACES, MS500, etc.
- Cybersecurity Community Leader @RedTeamRD
- HackTheBox Ambassador
- Twitter: @JulioUrena
- Blog: https://plaintext.do
- YouTube: https://www.youtube.com/c/JulioUreña






Agenda

- ❑ Introducción – ¿Porqué debemos probar nustras defensas?
- ❑ Red Team, Blue Team & Purple Team
- ❑ Purple Team Framework (PTEF)
- ❑ Simulación de ataques
- ❑ Frameworks para simulación de ataques
- ❑ MITRE ATT&CK® Framework
- ❑ Ejemplos prácticos de uso del MITRE ATT&CK® Framework
- ❑ Atomic Red Team
- ❑ Laboratorio
- ❑ Preguntas y Respuestas

¿Porqué deberíamos probar nuestras defensas?

Fuente: https://www.youtube.com/watch?v=hFZFjoX2cGg


https://www.youtube.com/watch?v=hFZFjoX2cGg

Cybersecurity Reference Architecture

May 2018 – https://aka.ms/MCRA | Video Recording | Strategies

Security Operations Center (SOC)

- Vulnerability Management
- MSSP
- SIEM + Analytics
- Cybersecurity Operations Service (COS)
- Incident Response and Recovery Services
- Azure Security Center
- Windows Defender
- Office 365 Security & Compliance
- Azure
- Cloud App Security
- Advanced Threat Protection (ATP)
- Graph Security API *(Public Preview)*
- Alert & Log Integration

This is interactive!

1. Present Slide
2. Hover for Description
3. Click for more information

Roadmaps and Guidance

1. Securing Privileged Access
2. Office 365 Security
3. Rapid Cyberattacks (Wannacrypt/Petya)

Software as a Service

Office 365

- Secure Score
- Customer Lockbox

Dynamics 365

Identity & Access

- Azure Active Directory
- Conditional Access – Identity Perimeter Management
- Azure AD Identity Protection
  - Leaked cred protection
  - Behavioral Analytics
- Azure AD PIM
- Multi-Factor Authentication
- Azure AD B2B
- Azure AD B2C
- Hello for Business
- MIM PAM
- Azure ATP
- Active Directory
- ESAE Admin Forest

Information Protection

- Cloud App Security
- Azure Information Protection (AIP)
  - Discover
  - Classify
  - Protect
  - Monitor
  - *Hold Your Own Key (HYOK)*
  - AIP Scanner
- Classification Labels
- Office 365
  - Data Loss Protection
  - Data Governance
  - eDiscovery
- Azure SQL Threat Detection
- SQL Encryption & Data Masking
- Azure SQL Info Protection *(Preview)*
- Endpoint DLP

Clients

Unmanaged & Mobile Devices

- Intune MDM/MAM

Managed Clients

- System Center Configuration Manager
- Windows Defender ATP
  - Secure Score
  - Threat Analytics

Hybrid Cloud Infrastructure

On Premises Datacenter(s) | 3rd party IaaS | Microsoft Azure

Azure Security Center – Cross Platform Visibility, Protection, and Threat Detection

- Configuration Hygiene
- Just in Time VM Access
- Adaptive App Control

Extranet

- NGFW
- Edge DLP
- SSL Proxy
- IPS

Security Appliances

Express Route

Intranet Servers

- Windows Server 2016 Security
  Window 10 + Just Enough Admin, Hyper-V Containers, Nano server, and more...
- Shielded VMs
- Azure Stack
- VMs

Privileged Access Workstations (PAWs)

- Azure Policy
- Azure Key Vault
- Azure WAF
- Azure Antimalware
- Application & Network Security Groups
- Backup & Site Recovery
- Disk & Storage Encryption
- Confidential Computing
- DDoS attack Mitigation+Monitor

Windows 10 Enterprise Security

- Network protection
- Credential protection
- Exploit protection
- Reputation analysis
- Full Disk Encryption
- Attack surface reduction
- App control
- Isolation
- Antivirus
- Behavior monitoring

S Mode

IoT and Operational Technology

- Windows 10 IoT
- Azure IoT Security
- Azure Sphere
- IoT Security Maturity Model
- IoT Security Architecture

Included with Azure (VMs/etc.) Premium Security Feature

Compliance Manager

Security Development Lifecycle (SDL)

Trust Center | Intelligent Security Graph

Microsoft

Equipos de Ciberseguridad

Red Team

Son profesionales de la seguridad ofensiva que son expertos en atacar sistemas e irrumpir en las defensas. Simula ataques para probar la eficacia de la seguridad y del BlueTeam.

Purple Team

Es la combinación de ambos equipos. Es un grupo que se encarga de hacer ambas cosas, definir la Seguridad y realizar las pruebas para medir la eficacia de ellas.

Blue Team

Son profesionales de seguridad defensiva responsables de mantener las defensas de la red interna contra todos los ataques y amenazas cibernéticos.

Purple Team Framework (PTEF)

En un nivel alto, se ejecuta un ejercicio de Purple Team con el siguiente flujo:

- La inteligencia de amenazas cibernéticas, el coordinador del RedTeam presentan al adversario, los TTP y los detalles técnicos.
- Los asistentes tienen una discusión sobre los controles de seguridad y las expectativas de TTP.
- Red Team emulates the TTP.
- Blue Team (SOC, Hunt team, and DFIR) los analistas siguen el proceso para detectar y responder a TTP.
- Documentación, realización de cambios de los controles de seguridad, revisión de eficacia de los cambios, documentar lecciones aprendidas.

https://www.scythe.io/ptef

Ejercicio de Purple Team es una actividad en el que los ataques se exponen y se explica al BlueTeam a medida que ocurre. Son ejercicios prácticos en los que el Blue/Red Team trabajan juntos con una discusión abierta sobre cada técnica de ataque y expectativa de defensa para mejorar las personas, los procesos y la tecnología en tiempo real.

¿Qué probar? ¿Qué simular?

Simulaciones:

- Ingeniería social - Personas, Procesos.
- Efectividad de soluciones de seguridad:
  - Antivirus / EDR.
  - Firewalls.
  - Email Gateway.
- Capacidad de respuesta a incidentes.
- Capacidad de colección de data.
- Tiempo de respuesta a un incidente.

Foco en el negocio es importante conocer el negocio y a qué se dedica la empresa y cuales elementos tecnológicos representan mayor impacto a la organización.

Frameworks de Simulación de Ataques

Gratis

- APT Simulator
- Atomic Red Team
- Caldera
- Purple Sharp
- Blue Team Training Toolkit
- Unfetter
- Entre otros

Comerciales

- Office 365 Attack Simulator
- AttackIQ
- Cymulate
- SafeBreach
- RanSim
- Madiant Advantage
- Entre otros

Simulación de Ataques le permite ejecutar simulaciones benignas de ciberataques en su organización para probar sus políticas y prácticas de seguridad, así como capacitar a sus empleados para aumentar su conciencia y disminuir su susceptibilidad a los ataques.

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training

Una mirada más de cerca a los Frameworks

Atomic Red Team

UNFETTER

PurpleSharp

Attack Frameworks existen diferentes Frameworks de simulación de ataques y adversarios que buscan automatizar el proceso de pruebas de soluciones y estrategias de ciberseguridad.

MITRE ATT&CK® Framework

MITRE ATT&CK® es una base de conocimiento accesible a nivel mundial de tácticas y técnicas utilizadas por los adversarios basadas en observaciones del mundo real. La base de conocimientos de ATT&CK se utiliza como base para el desarrollo de modelos y metodologías de amenazas específicas en el sector privado, en el gobierno y en la comunidad de productos y servicios de ciberseguridad.

https://attack.mitre.org/

MITRE se dedica a resolver problemas para un mundo más seguro. Trabajamos en el interés público para descubrir nuevas posibilidades, crear oportunidades inesperadas y liderar siendo pioneros juntos por el bien público para hacer realidad ideas innovadoras.

https://www.mitre.org/about/corporate-overview

MITRE ATT&CK® Framework

MITRE ATT&CK® organiza estos comportamientos en una serie de tácticas: "Objetivos técnicos específicos que un atacante quiere lograr":

- Reconocimiento.
- Acceso Inicial.
- Ejecución.
- Persistencia.
- Evasión de Defensas.
- Movimiento Lateral.
- Exfiltración.

Dentro de cada **táctica** hay diferentes **técnicas**.

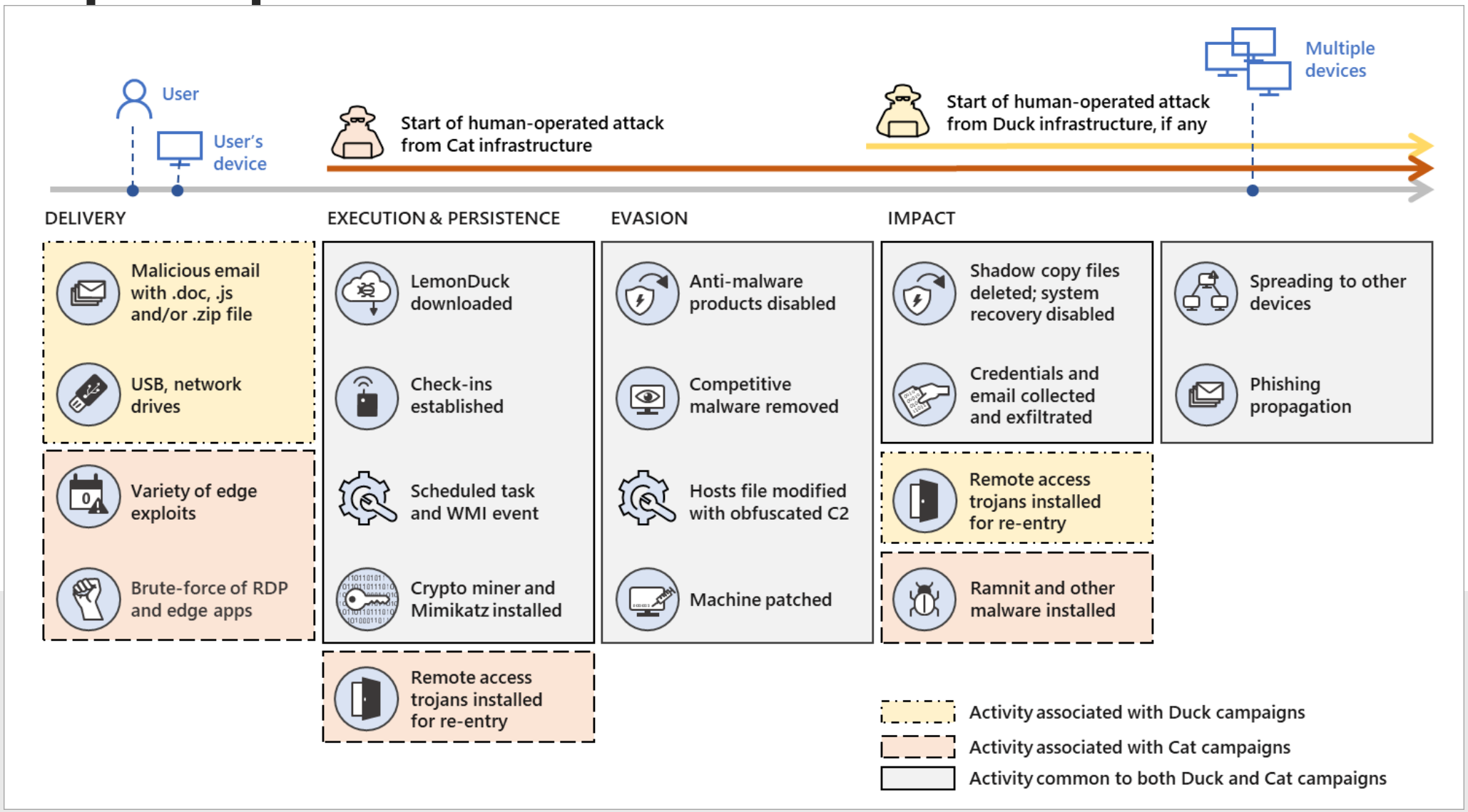
ATT&CK® te ayuda a entender cómo los atacantes operan, de modo que puedas comprenderlo y planificar cómo podrías detectarlos o prevenirlos.

MITRE ATT&CK® Framework

https://attack.mitre.org/

Arriba están las **tácticas** y **técnicas** que representan la matriz **MITRE ATT&CK®** para empresas. Matrix contiene información para las siguientes plataformas: Windows, macOS, Linux, PRE, Azure AD, Office 365, Google Workspace, SaaS, IaaS, Red, Contenedores.

Ejemplos prácticos del MITRE ATT&CK®



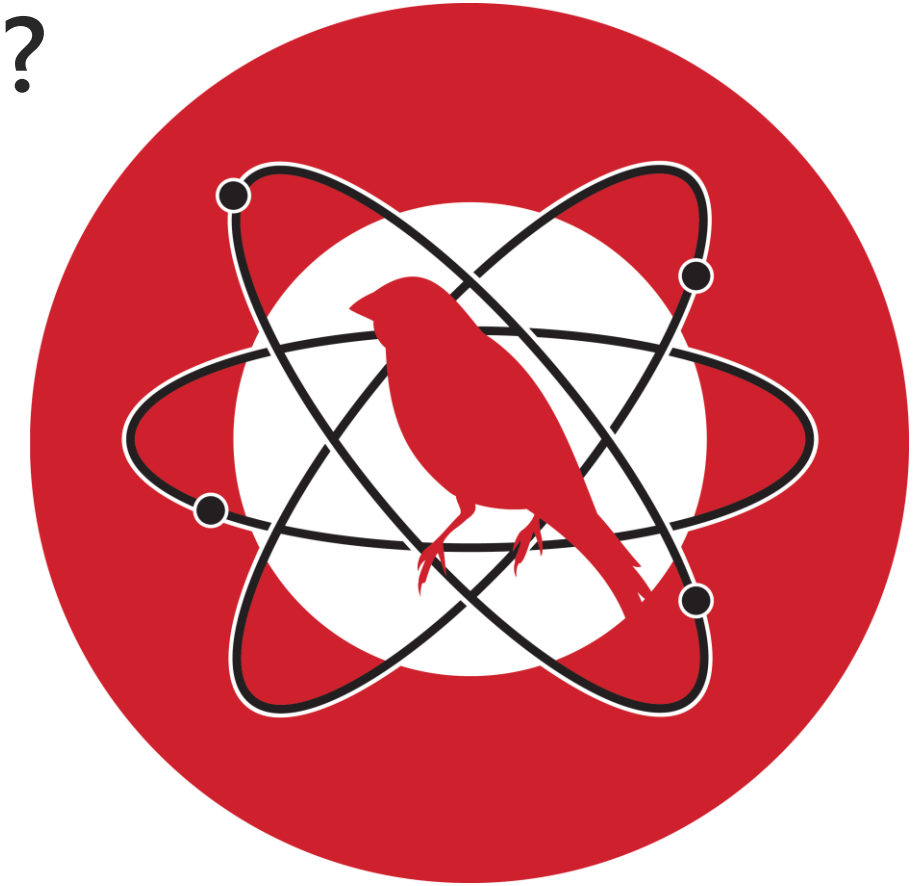
LemonDuck and LemonCat: Modern mining malware

Laboratorio
Probando Los Frameworks

¿Qué es el Atomic Red Team?

Conoce la familia de Atomic Red Team

- Atomic Red Team
- Invoke-Atomic
- AtomicTestHarnesses
- Chain Reactor



slack

https://slack.atomicredteam.io/

Atomic Red Team es una biblioteca de pruebas sencillas que todo equipo de seguridad puede ejecutar para probar sus defensas. Las pruebas están enfocadas, tienen pocas dependencias y se definen en un formato estructurado que puede ser utilizado por marcos de automatización.

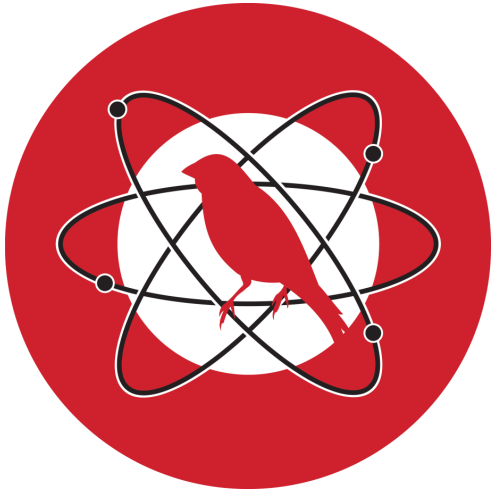
https://atomicredteam.io/

Invoke-Atomic

Prerequisitos

- Asegurate de tener permisos para correr las pruebas.
- Ejecuta las pruebas en un ambiente controlado.
- Instalar Powershell 5.0 o superior.

Enlace:
https://github.com/redcanaryco/invoke-atomicredteam



Invoke-Atomic es un módulo de PowerShell para desarrollar y ejecutar pruebas utilizando el Atomic RedTeam Framework. Con PowerShell Core, los equipos de seguridad pueden ejecutar pruebas en múltiples plataformas y en la red.

https://atomicredteam.io/

PurpleSharp

La telemetría de ataques producida por técnicas de simulación con PurpleSharp ayuda a los equipos de investigación y detección en:

- Construyendo nuevas analíticas de detección
- Prueba de análisis de detección existentes
- Validación de la resiliencia de la detección
- Identificar ausencia de visibilidad

https://www.purplesharp.com/en/latest/
https://github.com/mvelazc0/PurpleSharp
https://github.com/mvelazc0/PurpleAD

PurpleSharp

PurpleSharp es una herramienta de simulación de adversarios de código abierto escrita en C # que ejecuta técnicas de adversarios en entornos de Windows Active Directory. La telemetría resultante se puede aprovechar para medir y mejorar la eficacia de un programa de ingeniería de detección.

Recomendaciones

- Entender su infraestructura, procesos, sistema, negocio.
- Comprender la naturaleza del negocio/organización y definir pruebas de seguridad que beneficien el negocio.
- Familiarizarse con el MITRE ATT&CK Framework.
- Apoyarse en organizaciones con madurez en ejercicios de Pentesting y/o Redteam para crear ejercicios de PurpleTeam utilizando el Purple Team Framework.
- Crear ejercicios de RedTeam / PurpleTeam.
- No creer en todo lo que les dicen, hagan sus pruebas.

¿Preguntas?