US ProTech
CYBER SECURITY

US ProTech, founded in 1999, has many accomplishments:

Validated by The U.S. Dept. of Commerce Under N.I.S.T.
Exceeds U.S. Military High Impact Baseline Standards
Saved Clients over 200 Million in Cyber Liability & Risk
Manages Over 25 Billion Dollars in Assets and Info
Global Presence Throughout the America's & Europe
Int'l Government Contracts / Presidential Administrations

- Incident Forensics
- Firewall management
- Behavioral Monitoring
- Managed infrastructure
- Network based IPS / IDS
- Vulnerability Assessments
- Cyber-Security Assessments
- Endpoint /End user security
- Data Loss Prevention (DLP)
- Data Breach Risk Intelligence
- Security & Threat intelligence
- APT detection and remediation
- Log management & monitoring
- Email: encryption, spam filtering
- DDoS Red-Team Response Service
- Offensive-Side Penetration Testing
- Cyber Financial Liability Assessment
- Remote Managed Security Monitoring
- Server & Endpoint patch management
- Security info event management (SIEM)
- Governance, Risk, & Compliance (GRC)
- Critical Incident Response Team / CIRT
- Identity and access management services

US ProTech
CYBER SECURITY

2014 - 2018
Awarded Foreign Presidential Administration multi-year cyber security services contract

2015
Honor Award: Global Top 20 RSA Security Solution Providers

2016
Honor Award: Global Top 20 Leading Cyber Security Providers

2016
Honor Award: Global Top 20 Compliance Solution Providers

U.S. DEPARTMENT OF COMMERCE
BUREAU OF INDUSTRY AND SECURITY

US ProTech Cyber Services are Validated by the US DOC to exceed US Military standards under N.I.S.T. and is SCAP Approved.

US ProTech
CYBER SECURITY

UNDERSTANDING THE 7 STEPS OF THE CYBER-SECURITY KILL CHAIN

Newport Beach, CA • Las Vegas, NV
(949) 629-3900 • www.USProTech.com

1. RECONNAISSANCE: Identify the Targets

ADVERSARY: The adversaries are in the planning phase of their operation. They conduct research to understand which targets will enable them to meet their objectives.

DEFENDER: Detecting reconnaissance as it happens can be very difficult, but when defenders discover recon – even well after the fact – it can reveal the intent of the adversaries.

2. WEAPONIZATION: Prepare the Operation

ADVERSARY: The adversaries are in the preparation and staging phase of their operation. Malware generation is likely not done by hand – they use automated tools. A "weaponizer" couples malware and exploit into a deliverable payload.

DEFENDER: This is an essential phase for defenders to understand. Though they cannot detect weaponization as it happens, they can infer by analyzing malware artifacts. Detections against weaponizer artifacts are often the most durable & resilient defenses.

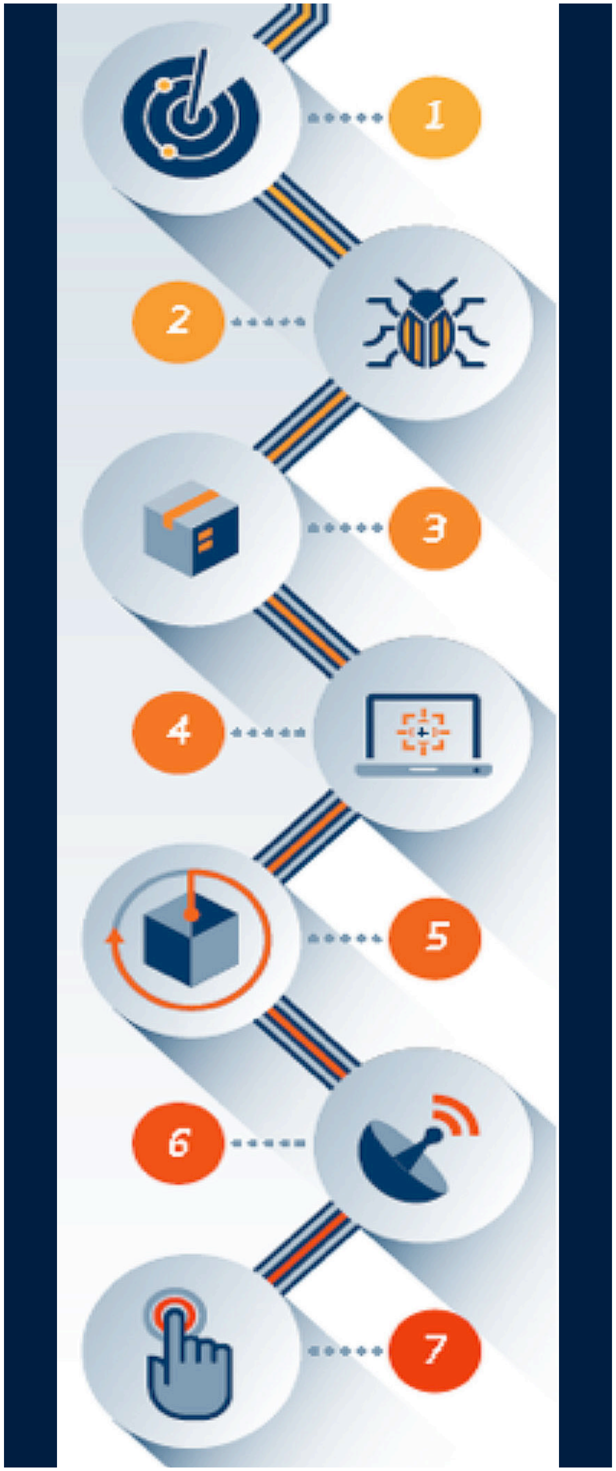
3. DELIVERY: Launch the Operation

ADVERSARY: The adversaries convey the malware to the target. They have launched their operation.

DEFENDER: This is the first and most important opportunity for defenders to block the operation. A key measure of effectiveness is the fraction of intrusion attempts that are blocked at delivery stage.

4. EXPLOITATION: Gain Access to the Victim

ADVERSARY: The adversaries must exploit a vulnerability to gain access. The phrase "zero day" refers to the exploit code used in just this step.



DEFENDER: Here traditional hardening measures add resiliency, but custom capabilities are necessary to stop zero-day exploits at this stage.

5. INSTALLATION: Establish Beachhead at the Victim

ADVERSARY: Typically, the adversaries install a persistent backdoor or implant in the victim environment to maintain access for an extended period of time.

DEFENDER: Endpoint instrumentation to detect and log installation activity. Analyze installation phase during malware analysis to create new endpoint mitigations.

6. COMMAND & CONTROL (C2): Remotely Control the Implants

ADVERSARY: Malware opens a command channel to enable the adversary to remotely manipulate the victim.

DEFENDER: The defender's last best chance to block the operation: by blocking the C2 channel. If adversaries can't issue commands, defenders can prevent impact.

7. ACTIONS ON OBJECTIVES: Achieve the Mission's Goals

ADVERSARY: With hands-on keyboard access, intruders accomplish the mission's goal. What happens next depends on who is on the keyboard.

DEFENDER: The longer an adversary has C2 access, the greater the impact. Defenders must detect this stage as quickly as possible by using forensic evidence – including network packet captures, for damage assessment.

US ProTech would like to thank our partners for their contribution to our presentation: Lockheed Martin • SANS Institute • University of California Los Angeles