Secure Programming

A.A. 2022/2023

Corso di Laurea in Ingegneria delle Telecomnicazioni

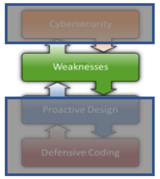
C. SwA: Weakness, Vulnerability, Attacks

Paolo Ottolino

Politecnico di Bari

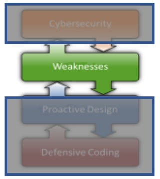
DIPARTIMENTO DI
INGEGNERIA ELETTRICA
E DELL'INFORMAZIONE

Secure Programming Lab: Course Program



A. **Intro Secure Programming: «Who-What-Why-When-Where-How»**
B. **Building Security in: Buffer Overflow, UAF, Command Inection**
C. **SwA: Weaknesses, Vulnerabilities, Attacks**
D. **SwA (Software Assurance): Vulnerabilities and Weaknesses (CVE, OWASP, CWE)**
E. **Security & Protection: Risks, Attacks. CIA -> AAA (AuthN, AuthZ, Accounting) -> IAM, SIEM, SOAR**
F. **Architecture and Processes: App Infrastructure, Three-Tiers, Cloud, Containers, Orchestration**
G. **Architecture and Processes 2: Ciclo di Vita del SW (SDLC), DevSecOps**
H. **Dynamic Security Test: VA, PT, DAST (cfr. VulnScanTools), WebApp Sec Scan Framework (Arachni, SCNR)**
I. **Free Security Tools: OWASP (ZAP, ESAPI, etc), NIST (SAMATE, SARD, SCSA, etc), SonarCube, Jenkins**
J. **Architecture and Processes 3: OWASP DSOMM, NIST SSDF**
K. **Operating Environment: Kali Linux on WSL**
L. **Python: Powerful Language for easy creation of hacking tools**
M. **Exercises: SecureFlag**

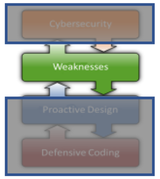
SwA: Software Assurance



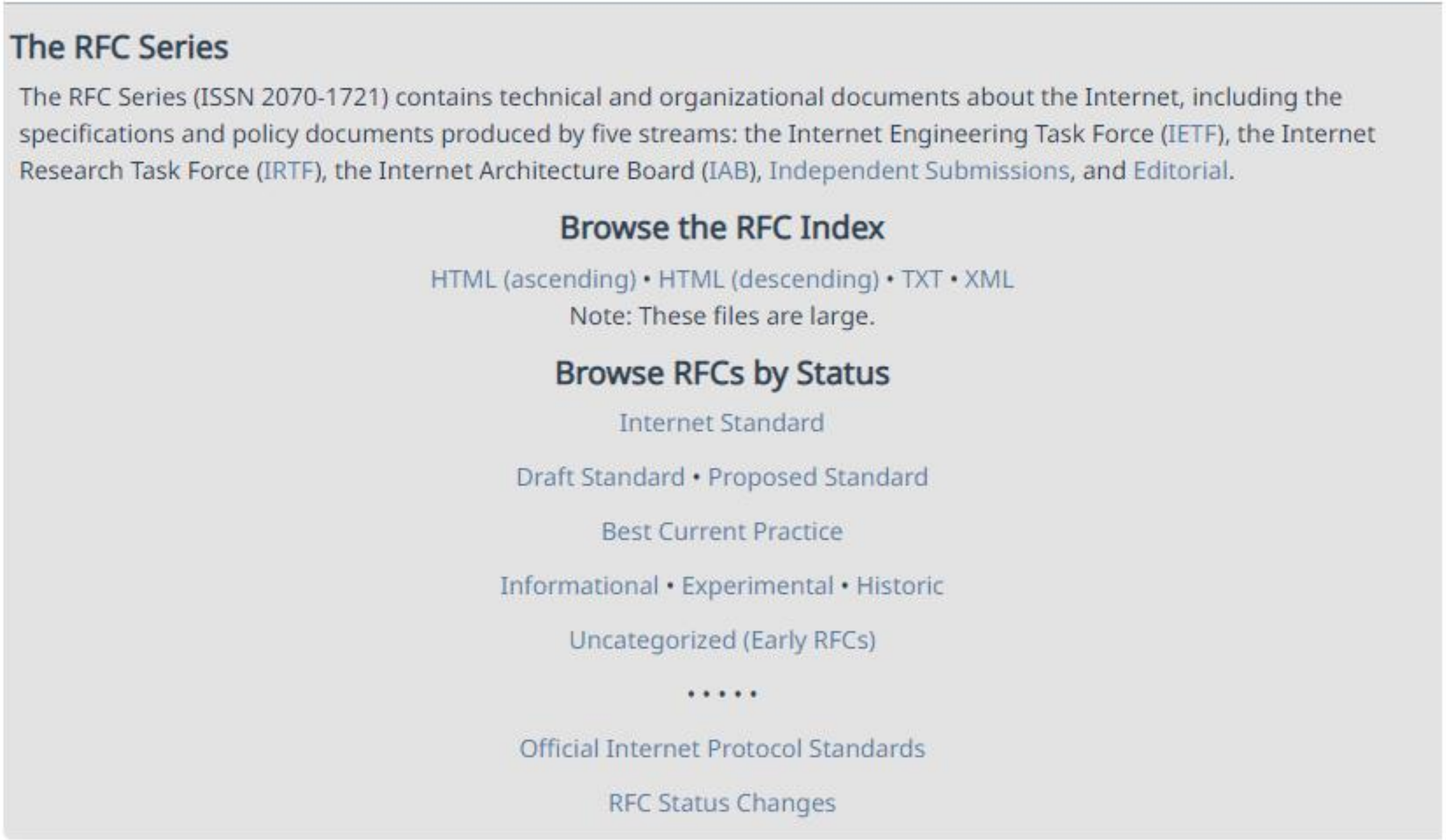
1. **Weakness**: Glossary
2. **Cyber Kill Chain**: Attacks Life Cycle
3. **Attacks and Vulnerabilities**: Security Bullettin

C.1 Weaknesses: Glossary

Internet Security Glossary 1/3



Concepts and definitions taken from RFC 4949 (update of RFC2828)



The RFC Series

The RFC Series (ISSN 2070-1721) contains technical and organizational documents about the Internet, including the specifications and policy documents produced by five streams: the Internet Engineering Task Force (IETF), the Internet Research Task Force (IRTF), the Internet Architecture Board (IAB), Independent Submissions, and Editorial.

Browse the RFC Index

HTML (ascending) • HTML (descending) • TXT • XML

Note: These files are large.

Browse RFCs by Status

Internet Standard

Draft Standard • Proposed Standard

Best Current Practice

Informational • Experimental • Historic

Uncategorized (Early RFCs)

• • • • •

Official Internet Protocol Standards

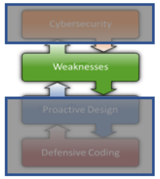
RFC Status Changes

The RFC series has a long history. The series was originated in 1969 by Steve Crocker of UCLA, to organize the working notes of the new ARPAnet research program. Online data access (e.g., FTP) was defined in early RFCs, and the RFC series itself became the first online publication series. For 28 years, this RFC series was managed and edited by the Internet pioneer Jon Postel. The RFC Editor operation was funded by the Defense Advanced Research Projects Agency (DARPA) of the US government until 1998. From 1998 – 2018, the RFC Editor was funded by a contract with the Internet Society, to continue to edit, publish, and catalog RFCs.

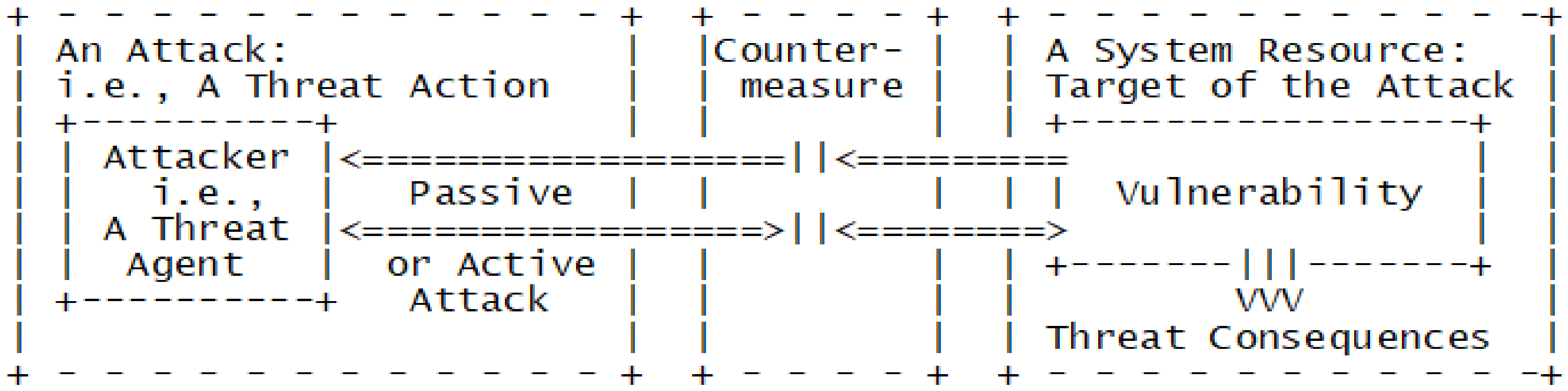
RFC 4949 “Internet Security Glossary https://www.rfc-editor.org/rfc/rfc4949

C.1a Weaknesses: Glossary

Internet Security Glossary 2/3



Concepts and definitions taken from RFC 4949 (update of RFC2828)



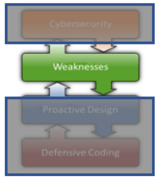
```
+ - - - - - - - - - - - - +  + - - - - +  + - - - - - - - - - - -+
| An Attack:              |  |Counter- |  | A System Resource:   |
| i.e., A Threat Action   |  | measure |  | Target of the Attack |
| +----------+            |  |         |  | +-----------------+  |
| | Attacker |<==================||<=========                 |  |
| |   i.e.,  |   Passive  |  |         |  | |  Vulnerability  |  |
| | A Threat |<=================>||<========>                 |  |
| |  Agent   |  or Active |  |         |  | +-------|||-------+  |
| +----------+   Attack   |  |         |  |         VVV          |
|                         |  |         |  | Threat Consequences  |
+ - - - - - - - - - - - - +  + - - - - +  + - - - - - - - - - - -+
```

Attacco (Attack): Intentional act, by which an attempt is made to evade the security controls of a system and violate its security policies.
Azione di Minaccia (Threat Action): Effective Assault on a security system.
Agente di Minaccia (**Threat Agent**): the one who carries out the attack (Attacker)
Minaccia (**Threat**): Potential breach of security, which exists in the presence of a circumstance, skill, action, or event that could violate security and cause harm.
Contromisura (Countermeasure): Action, device, procedure, or technique that reduces a threat, vulnerability, or attack by eliminating or preventing it, minimizing the harm it may cause, or discovering and reporting it so that corrective action can be taken.

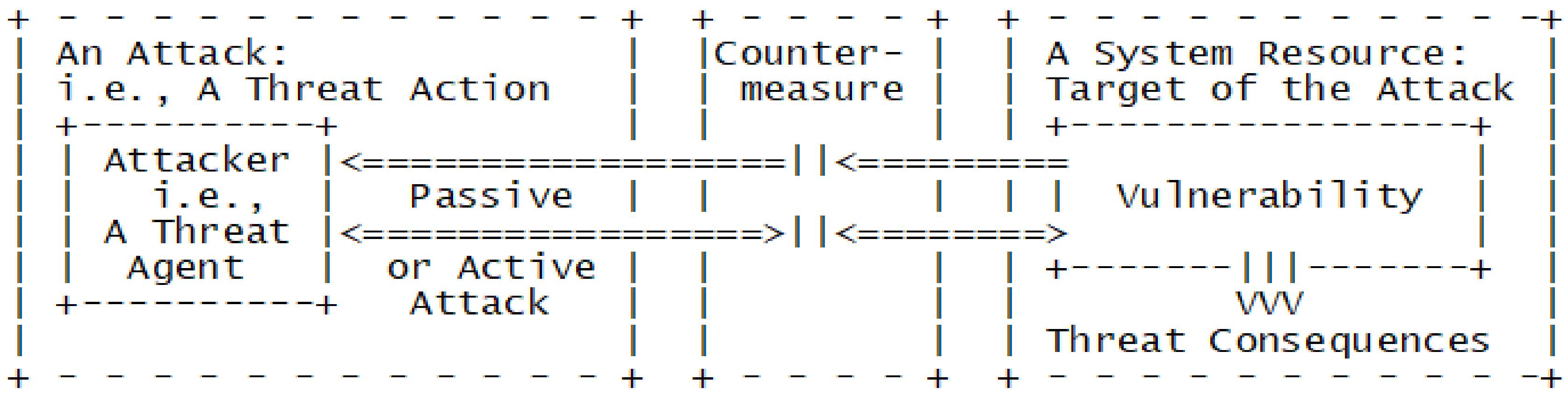
RFC 4949 “Internet Security Glossary https://www.rfc-editor.org/rfc/rfc4949

C.1b Weaknesses: Glossary

Glossary 3/3



Concepts and definitions taken from RFC 4949 (update of RFC2828)



```
+ - - - - - - - - - - - - - +  + - - - - +  + - - - - - - - - - - -+
| An Attack:                |  |Counter- |  | A System Resource:   |
| i.e., A Threat Action     |  | measure |  | Target of the Attack |
| +----------+              |  |         |  | +-----------------+  |
| | Attacker |<==================||<=========                 |  |
| |   i.e.,  |   Passive    |  |         |  | |  Vulnerability  |  |
| | A Threat |<=================>||<========>                 |  |
| |  Agent   |  or Active   |  |         |  | +-------|||-------+  |
| +----------+   Attack     |  |         |  |         VVV          |
|                           |  |         |  | Threat Consequences  |
+ - - - - - - - - - - - - - +  + - - - - +  + - - - - - - - - - - -+
```

Vulnerabilità (**Vulnerability**): Flaw or weakness in the design, implementation, or operation and management of a system that could be exploited to violate system security policies.

Conseguenza di Minaccia (**Threat Consequence**): A security breach resulting from a threat action. Includes:

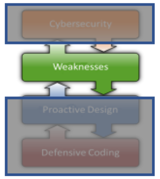
- Exfiltration/disclosure
- inganno (deception)
- denial/interruption
- usurpation

Rischio (Risk): loss perspective expressed as the probability that a given threat will exploit a given vulnerability with a given harmful result.

RFC 4949 “Internet Security Glossary https://www.rfc-editor.org/rfc/rfc4949

C.1c Weaknesses: Glossary

Glossary: Attack

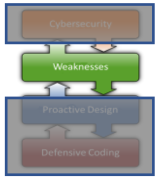


The attack is classified according to a number of attributes

Characterization	
Intent	• <u>Active</u>: alter system resources and modify its running operations • <u>Passive</u>: collect information from the system, without touching its resources
Stage	• <u>On-Line</u>: the information retrieval, analysis and application phases take place in rapid succession • <u>Off-Line</u>: The information obtained is analyzed on another system (typically owned by the attacker). Only after that, the results are applied on the target system
Initiation	• <u>Inside</u>: undertaken by an entity residing within (insider) the security perimeter • <u>Outside</u>: operated from outside the security perimeter, by an unauthorized user (outsider)
Delivery	• <u>Direct</u>: packets are sent directly to the intended victim • <u>Indirect</u>: the packets are sent to a third party, which sends them to the victim(s).

C.1d Weaknesses: Glossary

Glossary: Vulnerability



Vulnerability: Defect or weakness of a system that could be exploited to violate its security policy

Phase		Weakness
Design	(Specification): progettazione	Algorythm (es. MTProto, Telegram): - Weak hash algorithm - Mac & Encrypt (instead of Encrypt & Mac) - CBC variant (Infinite Garble Extension)(*) - No PubKeys authentication
Implementation	Realization	Code: - Input Validation - SQLi, XSS, CSRF, etc
Operation	Working	Esecution - ACL - External Object
Management	Governance (Command & Control)	Process: - Need to Know - Segregation od Duties - Due Care/Due Diligence - Awareness

(*) NIST SP800-38°: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf

C.1e Weaknesses: Glossary

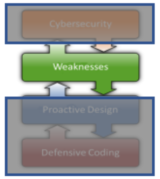
Glossary: Attack Vector

Careful analysis is required to convey an attack, breakthrough and 3 levels (Strategic, Tactical and Operational)

	eMail	Web	Chat	Physic
Strategic	Social Engineering	Intrigue	Enticement Hookup	Manipulation
Tactical	Phishing	Web vuln (es. XSS) Browser	Attach	USB Key
Operational	Payload (Executable / Script)			

C.1f Weaknesses: Glossary

Glossary: Threat Consequence



Various consequences can arise following a successful attack

Unauthorized Disclosure (divulgazione non autorizzata) - threat consequence: a circumstance or event in which an entity gains access to data for which it does not have permission (confidentiality).

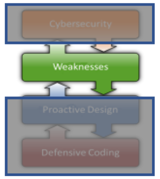
Deception (raggiro) - threat consequence: Circumstance or event that could result in an authorized entity receiving false (presumed to be true) data

Disruption (interruzione) - threat cons: circumstance or event that interrupts or prevents the correct operation of the services and functions of a system. (see Denial of Service)

Appropriation (usurpazione) - thread conseq: circumstance or event that results in the control of the services or functions of a system by an unauthorized entity.

C.1g Weaknesses: Glossary

Glossary: Unauthorized Disclosure 1/2



The following threat actions can cause unauthorized disclosure

Exposure (esposizione): a threat action in which sensitive data is directly released to an unauthorized entity.

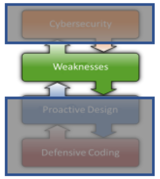
Voluntary Exposure: intentional release of data to unauthorized entities.
Scavenging: the act of "rummaging through" residual data in a system in search of sensitive information;
*Human Error: human action or negligence resulting in the inadvertent exposure of data to an unauthorized entity.
*Errore sw/hw. System failure resulting in unintentional data exposure to third parties.

Interception: a threat action in which an unauthorized party gains direct access to sensitive data in transit between authorized senders and recipients. It includes:

Theft: obtaining access to sensitive data through the theft of a physical medium (eg disk, CD, pendrive) in transit (eg shipment) containing the data.
Wiretapping (passive): Monitoring and logging of data in transit between two points in a communication system.
Emanation analysis: direct obtaining of information on data communicated through the monitoring and processing of a signal emitted by a system and containing the data, but not foreseen as a data communication system (cft emanation, TEMPEST?).

C.1h Weaknesses: Glossary

Glossary: Unauthorized Disclosure 2/2



The following threat actions can cause unauthorized disclosure

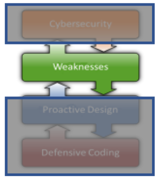
Inference: threat action in which an unauthorized entity indirectly accesses sensitive data (but not necessarily the data contained in the communication) through deduction from characteristics or byproducts of the communication. It includes:

- Traffic analysis: Obtaining insights into data by observing the characteristics of the communication carrying the data.
- Signal analysis: indirect obtaining of information on communicated data, through the monitoring and analysis of a signal emitted by a system and containing the data, but not intended as a means of communication of the same. (cft emanation).

Intrusion: threat action in which an unauthorized entity gains access to sensitive data by circumventing a system's protections. It includes:

- Physical Intrusion: Gaining unauthorized physical access to sensitive information by circumventing a system's safeguards.
- Penetration: Gaining logical access to sensitive data by circumventing a system's protections.
- Reverse Engineering: acquisition of sensitive data through the disassembly and analysis of the design of a system or a component of it.
- Cryptanalysis: the transformation of encrypted data into plaintext data without prior knowledge of encryption parameters or processes.

C.1i Weaknesses: Glossary



Glossary: Deception

The following threat actions can lead to the scam

"Masquerade": action in which an unauthorized party gains access to a system or performs malicious operations by posing as an authorized party.

- Spoof: Attempting to gain access to a system by posing as an authorized user.
- Malicious logic: In the context of masquerade, any hardware, firmware, or software (e.g. Trojan) that appears to provide useful and desirable functions, but instead gains unauthorized access to system resources or tricks the user into forcing him to execute other malicious logic. (cfg malicious logic)

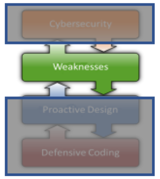
Forgery: thread action where false data misleads an authorized party (see active wiretapping)

- Substitution: Alteration or outright replacement of valid data with false data provided to an authorized party for the purpose of deceiving them.
- Insertion: introduction of false data with the aim of deceiving the receiving party.

Repudians/Repudiation: threat action in which one party deceives the other through the false repudiation of responsibility for an action. (see non-repudiatin service)

- False denial of origin: action in which the issuer of a data denies responsibility for the generation of the data itself.
- False denial of receipt: action in which the recipient of a data denies receipt and possession of the data

C.1j Weaknesses: Glossary



Glossary: Disruption

The following threat actions can cause disruption

Disabling (incapacitation): action that prevents or interrupts the operation of a service by disabling one of its components.

- Malicious logic: in this context, any hw, fw, sw (e.g. logic bomb) intentionally introduced into a system to destroy its functions or resources.
- Physical destruction: deliberate destruction of a component of a system with the aim of preventing its functioning.
- Human error: action or negligence that inadvertently leads to the disabling of a component.
- HW or SW error: an error that causes a system component to fail and leads to an interruption of operations.
- Natural Disaster: Natural disaster (fire, flood, lightning) that disables a system component.

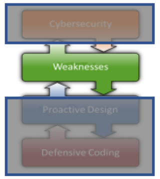
Corruption: action that undesirably impairs the operation of a system through the adverse modification of system functions or data.

- Tampering: In the context of corruption, the deliberate alteration of a system's logic, data, or control information to interrupt or prevent the proper operation of a system's functions.
- Malicious logic: any HW, FW or SW (e.g. virus) intentionally introduced into a system to modify its data or functionality.
- Human Error: Human action or negligence resulting in the inadvertent alteration of data or system functions.
- HW or SW error: Error resulting in corrupted data or functions.
- Natural Disaster: affecting operation or data.

Obstruction : threat action that interrupts the provision of system services by hindering/impeding/blocking system operation.

- Interference: disruption to operations resulting from blockage of communications or data.
- Overload: hindrance of the operation of a system through an excessive load to the detriment of the performance of the system or of one of its components (see flooding)

C.1k Weaknesses: Glossary



Glossary: Usurpation

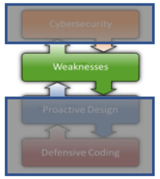
The following threat actions can cause usurpation

Misappropriation / embezzlement : action in which an entity assumes unauthorized access of a logical or physical type to a system or resources.

- service theft: unauthorized use of a service by an unauthorized entity
- Feature Theft: Unauthorized acquisition of hardware, software, or firmware of a system or component.
- data theft: unauthorized acquisition, and use, of data.

Misuse: action that causes a system or component to perform functions or services that are harmful to the system or its safety.

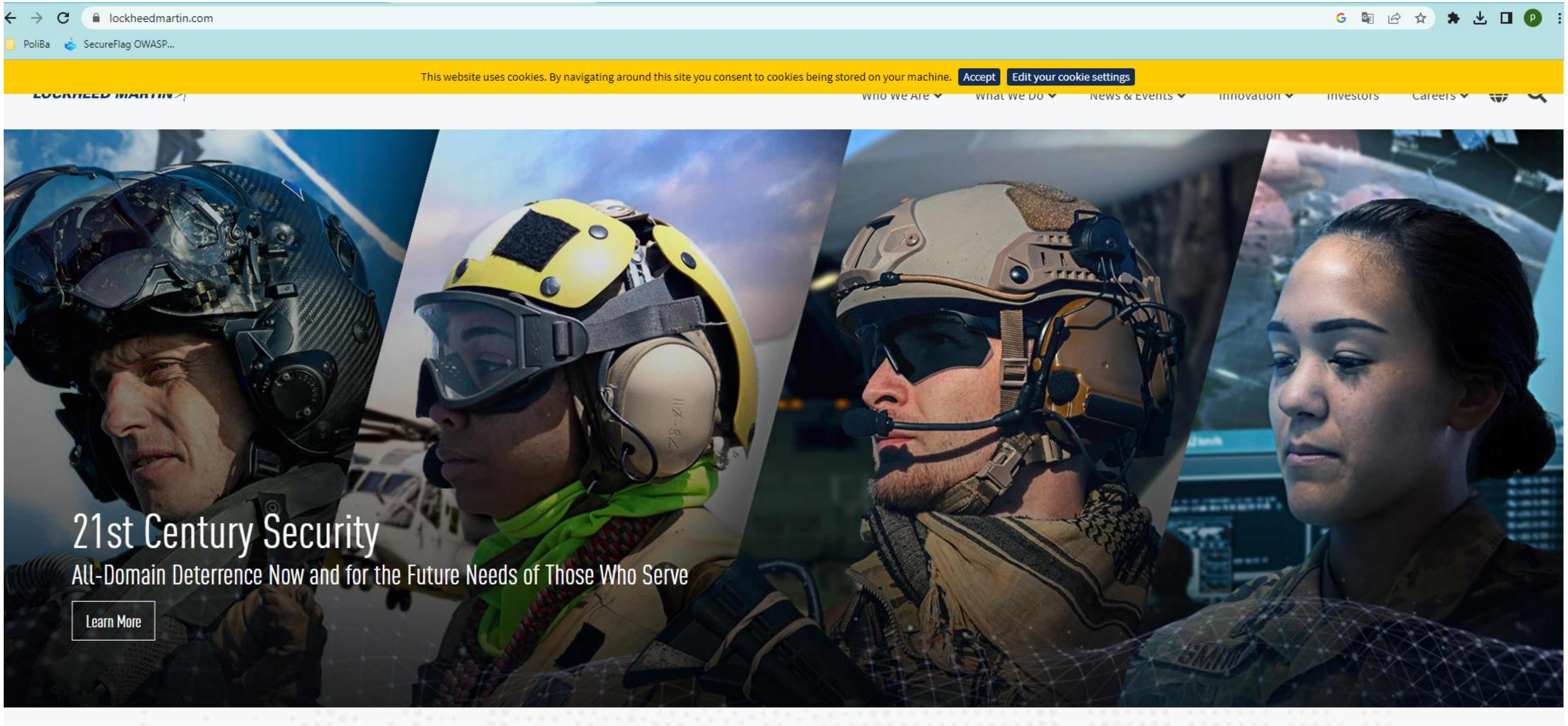
- Tampering: In the context of misuse, deliberately altering the logic, data or control information of a system to cause the system to perform unauthorized functions or services.
- Malicious logic: HW, FW or SW intentionally introduced into a system to perform or control the execution of unauthorized functions or services.
- Permission violation: action, performed by an entity, which exceeds the entity's privileges on the system by allowing the execution of unauthorized functions.



C.2a Attack Life Cycle: Cyber Kill Chain

Cyber Kill Chain 1/2

Concept transmuted from the military world by the Lockheed Martin company which owns the brand: each attack requires a life cycle



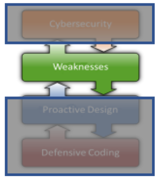
This website uses cookies. By navigating around this site you consent to cookies being stored on your machine.

21st Century Security

All-Domain Deterrence Now and for the Future Needs of Those Who Serve

C.2b Attack Life Cycle: Cyber Kill Chain

Cyber Kill Chain 1/3

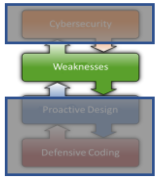


Concept transmuted from the military world by the Lockheed Martin company which owns the brand: each attack requires a life cycle

Reconnaissance	Identification, Selection and Profiling of the Target
Weaponization	Create the cyber weapon (contained in a payload), piecing together: • Trojan • Exploit
Delivery	Transmission of the cyber weapon to the target (tras' 'e sic)
Exploitation	Payload operation
Installazione	Installing a backdoor (t'e mett' 'e chiatt)
Command & Control	Establishing Client-Server communications with the compromised host
Act on Objective	• Data Exfiltration • Network Spreading • System Disruption

C.2c Attack Life Cycle: Cyber Kill Chain

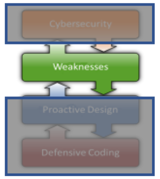
Cyber Kill Chain 2/3



Matrice degli Strumenti di Contrasto

Fase	Detect	Deny	Disrupt	Degrade	Deceive
Reconaissance	Web Analytics	FW AC			
Weaponization					
Delivery	Vigilant User NIDS (ATP)	Proxy Filter (WAF) NIPS (ATP)	AV (ATP)	Queueing	
Exploitation	HIDS (ATP)	Patch ACL	DEP ASLR		
Installation	HIDS (ATP)	Chroot (Container) ACL	AV (ATP)		
Command&Control	NIDS (ATP)	FW ACL	NIPS (ATP)	Tarpit	DNS redirect
Actions on Objectives	Audit Log (SIEM)			QoS	HoneyPot

C.2d Attack Life Cycle: Cyber Kill Chain



Cyber Kill Chain 3/3

Matrice degli Strumenti di Contrasto

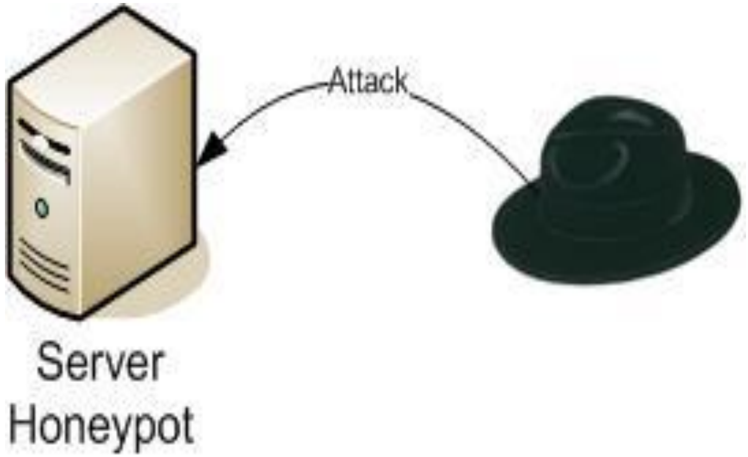
Acronym/Term	Meaning	Brief Description	Link
FW	FireWall	Filtering TCP/IP flows based on SRC, DST, port	
AC(L)	Access Control (List)		
Vigilant User	User aware of security issues	Awareness and Training	
NIDS / HIDS	N		
Proxy Filter (WAF)	Web Application Firewall		
AV (ATP)	Anti Virus (Advanced Threat Protection)	Detection of virus and malware by: • signatures • IoC (Index of Compromission) • Behavioural	
Patch	Security Update		
DEP	Data Execution Prevention	Prevent the execution of data	https://msrc.microsoft.com/blog/2010/12/on-the-effectiveness-of-dep-and-aslr/
ASLR	Address Space Layout Randomization	Load programs in not predictable locations	https://msrc.microsoft.com/blog/2010/12/on-the-effectiveness-of-dep-and-aslr/
Chroot (Container)	Change root	Changing the root (/) for a process	
Tarpit	Natural trap	Services on over unused IP addresses	https://labrea.sourceforge.io/Intro-History.html
QoS	Quality of Service		
DNS redirect	Domain Name System redirect	Fake resolutions of hostname	
Audit Log (SIEM)	Security Information and Event Management	Collection and correlation of (security) logs	https://www.gartner.com/reviews/market/security-information-event-management
HoneyPot			

C.2e Attack Life Cycle: Cyber Kill Chain

Server-side Attack

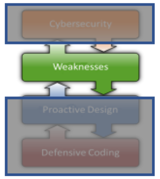
The perimeter is increasingly impenetrable: fortified and protected. Increasingly difficult to find a way to enter the victim's network.

Server side: directed to the assets in which the information of interest is contained (Espionage), whose resources you want to exploit (Proofitering) or that you want to damage (Damaging).



C.2f Attack Life Cycle: Cyber Kill Chain

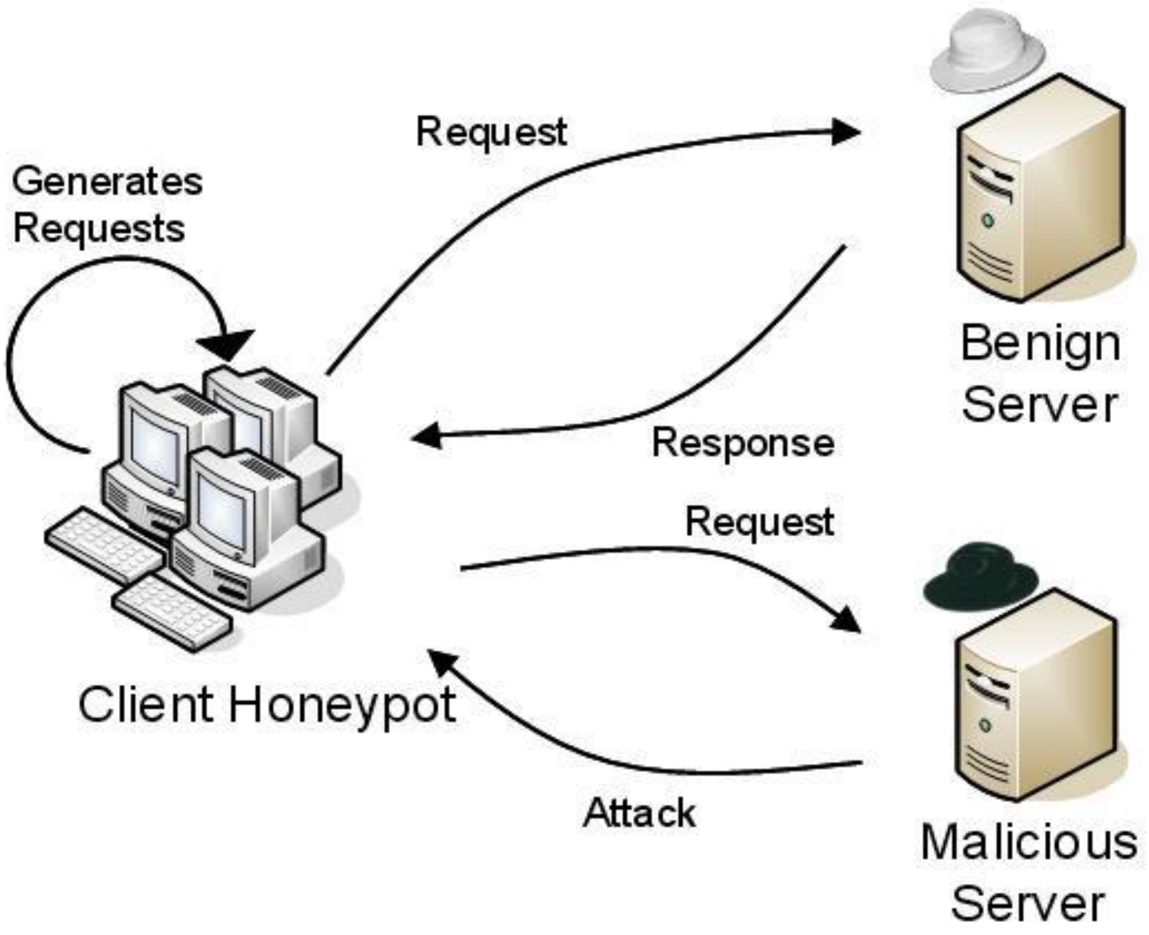
Client-side Attack 1/3



The perimeter is increasingly impenetrable: fortified and protected. This type of attack allows you to circumvent perimeters and fortifications.

Client side attacks:
Engage users and guide their interaction, such as:

- entice them to click on a link
- open a document
- get to your malicious site.

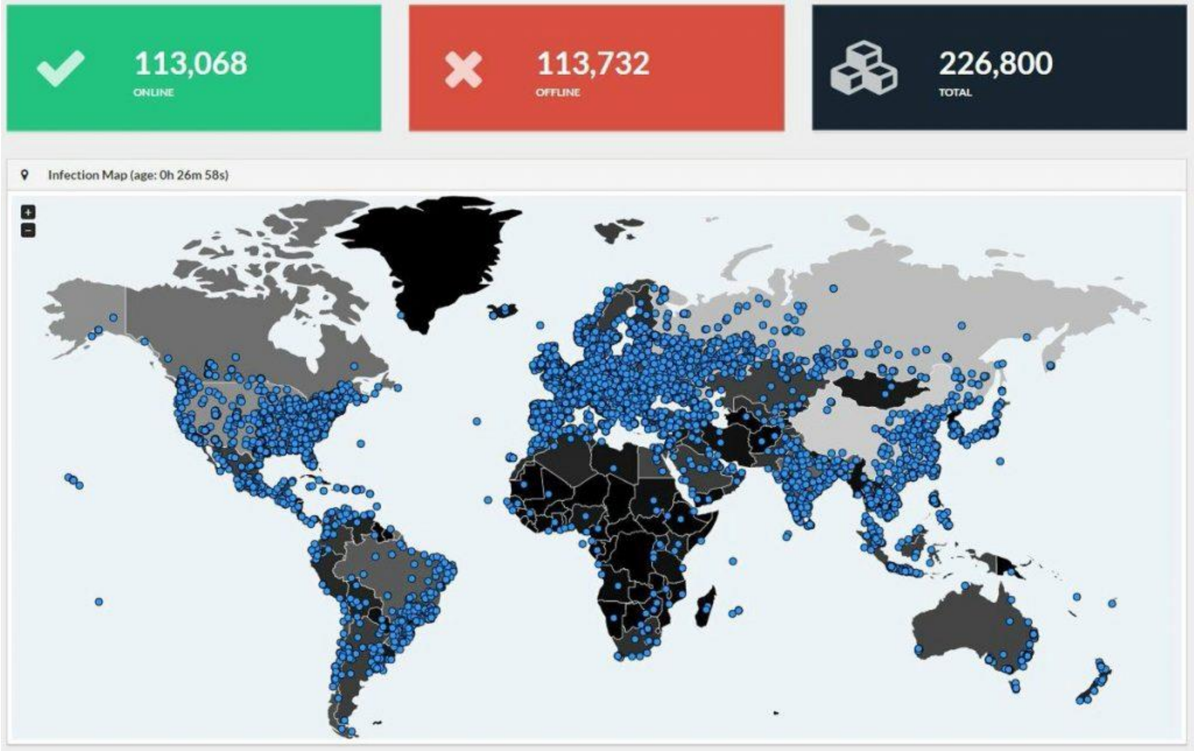


C.2g Attack Life Cycle: Cyber Kill Chain

Client-side Attack 2/3

It is known that people click on everything, if properly intrigued (primed)

Key Part: use social engineering skills to get the user to click



✓ 113,068 ONLINE

✗ 113,732 OFFLINE

226,800 TOTAL

Infection Map (age: 0h 26m 58s)

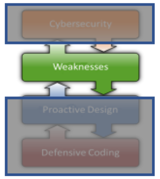
Malicious attack, on vulnerable services of a client machine, by means of :

- **Payload**: send malicious content
- **Trick**: entice the user to run the code
- **Reverse**: get a connection or a reverse-shell

Client side attacks are constantly increasing.

C.2h Attack Life Cycle: Cyber Kill Chain

Client-side Attack 3/3

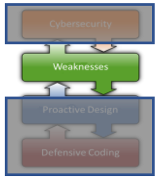


There are various ways to use tools initially designed for server-side attacks as well as for client-side attacks

	Content	Shape	Trick	Gain
Binary Linux Trojan	Linux Game	Ubuntu deb package	Convince to Install	Reverse Shell
Adobe Reader	‘util.printf()’ JavaScript Function Stack Buffer Overflow Vulnerability	PDF	Convince to Open	Reverse Shell
VBScript Infection	Office game	Docx Xlsx	Convince to Open	Meterpreter Shell

C.2i Attack Life Cycle: Cyber Kill Chain

Information Gathering



Finding useful information

Active:

- Contacts (rubrica)
- FingerPrint

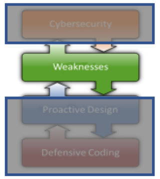
	Name	Version	Functions	other
Browser			Estensioni	
Mail Client			Conf.	
AV				
S.O.				

Passive

- Behavioural: Interactions (e.g. purchases) to be able to forge emails
- OSINT
- Links (firends, collegues, relatives)

C.2j Attack Life Cycle: Cyber Kill Chain

Evasion Techniques 1/2



Techniques to avoid being identified by End-Point protection systems

Identification of the Running System

SandBox: environment analysis

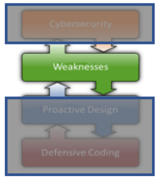
- CPU ID: identification of the running CPU
- MAC: addresses fo the virtual network interfaces
- Eth: identification of the names provided to the network interfaces (avoiding virtual environment))
- Registry: HKEY_LOCAL_MACHINE\HARDWARE\Description\System

SandBox: behavioural analysis

- HW Properties: low resolution, small HD, no 3D, etc
- SW: user clients (eMail, chat, etc)
- System: uptime
- User: desktop (clean), cookies (too few), FS (clean, no recent)
- DNS: «strange» hostname resolution (es. WannaCry)

C.2k Attack Life Cycle: Cyber Kill Chain

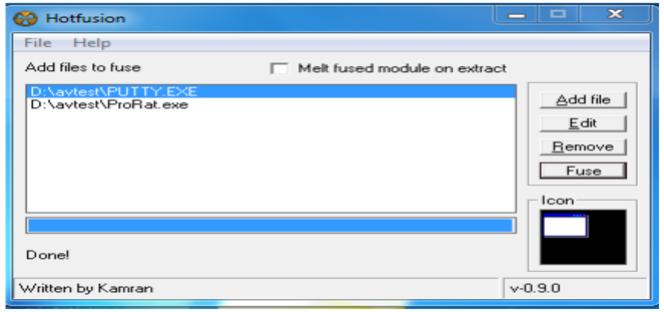
Evasion Techniques 2/2



Techniques to avoid being identified by End-Point protection systems

Deleting the Signature available in the AV

1. Binding and splitting (HotFusion)



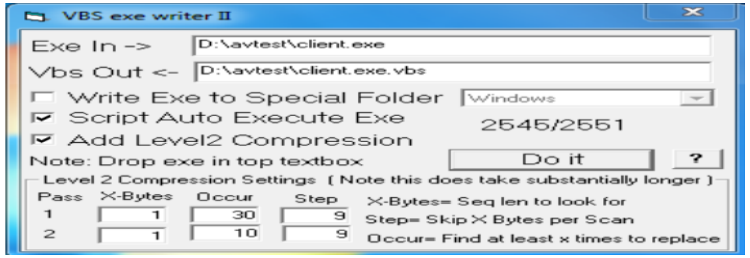
Add files to fuse

□ Melt fused module on extract

D:\avtest\PUTTY.EXE
D:\avtest\ProRat.exe

Done!

2. *.exe to ‘executable client side scripts’ (exe2vbs)



Exe In -> D:\avtest\client.exe

Vbs Out <- D:\avtest\client.exe.vbs

□ Write Exe to Special Folder   Windows

☑ Script Auto Execute Exe   2545/2551

☑ Add Level2 Compression

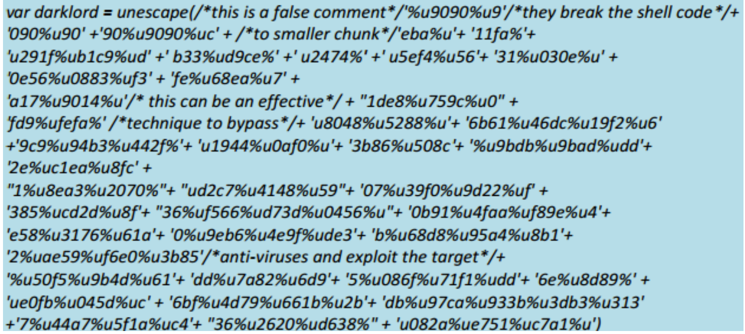
Note: Drop exe in top textbox

Level 2 Compression Settings (Note this does take substantially longer)

Pass	X-Bytes	Occur	Step
1	1	30	9
2	1	10	9

X-Bytes= Seq len to look for
Step= Skip X Bytes per Scan
Occur= Find at least x times to replace

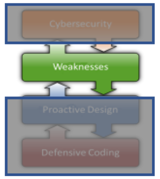
3. Code Obfuscation/Morphing

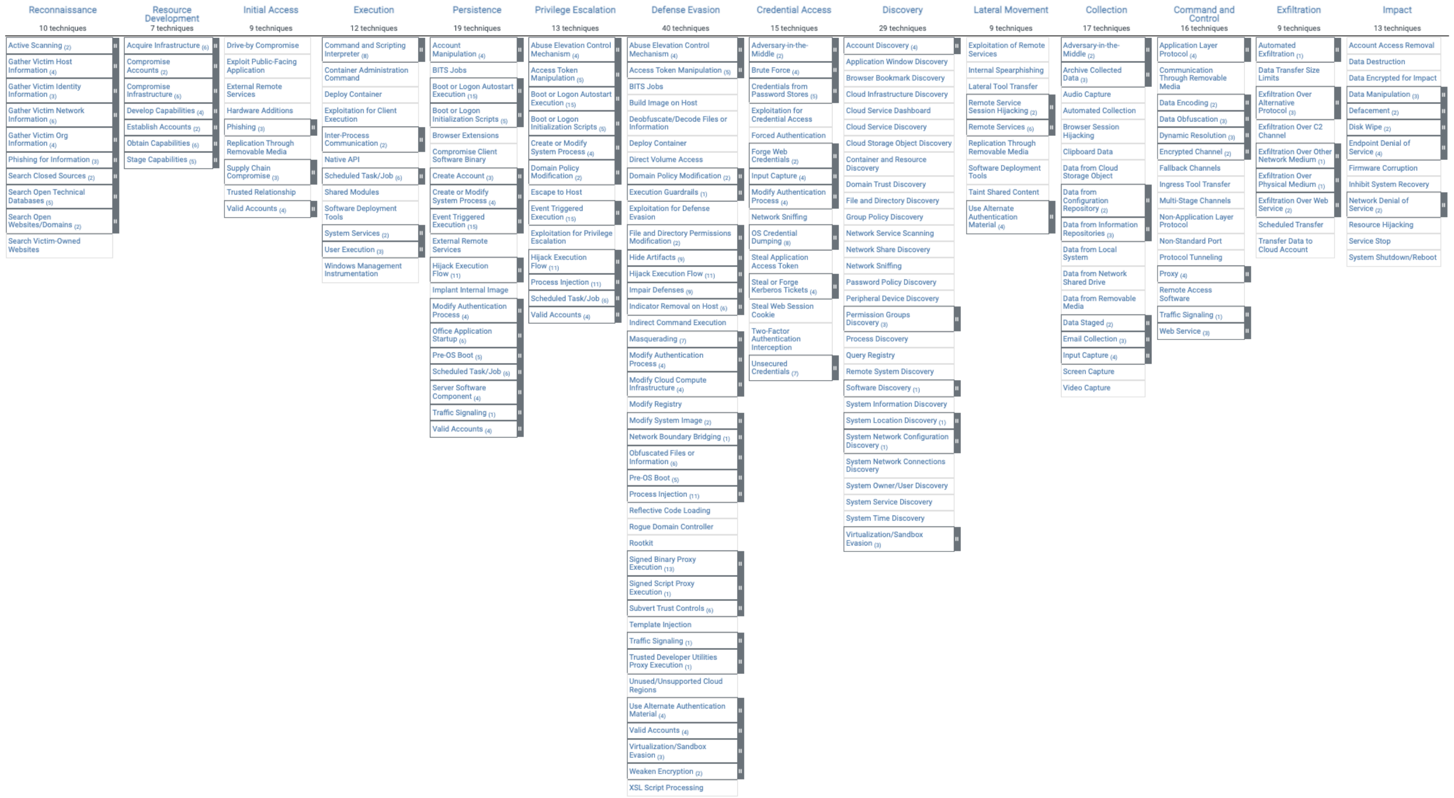


```
var darklord = unescape(/*this is a false comment*/'%u9090%u9'/*they break the shell code*/+
'090%u90' +'90%u9090%uc' + /*to smaller chunk*/'eba%u'+ '11fa%'+
'u291f%ub1c9%ud' +' b33%ud9ce%' +' u2474%' +' u5ef4%u56'+ '31%u030e%u' +
'0e56%u0883%uf3' + 'fe%u68ea%u7' +
'a17%u9014%u'/* this can be an effective*/ + "1de8%u759c%u0" +
'fd9%ufefa%' /*technique to bypass*/+ 'u8048%u5288%u'+ '6b61%u46dc%u19f2%u6'
+'9c9%u94b3%u442f%'+ 'u1944%u0af0%u'+ '3b86%u508c'+ '%u9bdb%u9bad%udd'+
'2e%uc1ea%u8fc' +
"1%u8ea3%u2070%"+ "ud2c7%u4148%u59"+ '07%u39f0%u9d22%uf' +
'385%ucd2d%u8f'+ "36%uf566%ud73d%u0456%u"+ '0b91%u4faa%uf89e%u4'+
'e58%u3176%u61a'+ '0%u9eb6%u4e9f%ude3'+ 'b%u68d8%u95a4%u8b1'+
'2%uae59%uf6e0%u3b85'/*anti-viruses and exploit the target*/+
'%u50f5%u9b4d%u61'+ 'dd%u7a82%u6d9'+ '5%u086f%u71f1%udd'+ '6e%u8d89%' +
'ue0fb%u045d%uc' + '6bf%u4d79%u661b%u2b'+ 'db%u97ca%u933b%u3db3%u313'
+'7%u44a7%u5f1a%uc4'+ "36%u2620%ud638%" + 'u082a%ue751%uc7a1%u')
```

C.2l Attack Life Cycle: Cyber Kill Chain

MITRE ATT&CK



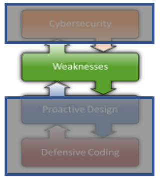


Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	40 techniques	15 techniques	29 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (2)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (2)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (15)	Boot or Logon Autostart Execution (15)	BITS Jobs	Credentials from Password Stores (5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (2)	Browser Extensions	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Services (6)	Browser Session Hijacking	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deploy Container	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (6)	Create Account (3)	Escape to Host	Direct Volume Access	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage Object	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)		Trusted Relationship	Shared Modules	Create or Modify System Process (4)	Event Triggered Execution (15)	Domain Policy Modification (2)	Modify Authentication Process (4)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment Tools	Event Triggered Execution (15)	Exploitation for Privilege Escalation	Execution Guardrails (1)	Network Sniffing	Domain Trust Discovery	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			System Services (2)	External Remote Services	Hijack Execution Flow (11)	Exploitation for Defense Evasion	OS Credential Dumping (8)	File and Directory Discovery		Data from Local System	Non-Application Layer Protocol		Network Denial of Service (2)
			User Execution (3)	Hijack Execution Flow (11)	Process Injection (11)	File and Directory Permissions Modification (2)	Steal Application Access Token	Group Policy Discovery		Data from Network Shared Drive	Non-Standard Port		Resource Hijacking
			Windows Management Instrumentation	Implant Internal Image	Scheduled Task/Job (6)	Hide Artifacts (9)	Steal or Forge Kerberos Tickets (4)	Network Service Scanning		Data from Removable Media	Protocol Tunneling		Service Stop
				Modify Authentication Process (4)	Valid Accounts (4)	Hijack Execution Flow (11)	Steal Web Session Cookie	Network Share Discovery		Data Staged (2)	Proxy (4)		System Shutdown/Reboot
				Office Application Startup (6)		Impair Defenses (9)	Two-Factor Authentication Interception	Network Sniffing		Email Collection (3)	Remote Access Software		
				Pre-OS Boot (5)		Indicator Removal on Host (6)	Unsecured Credentials (7)	Password Policy Discovery		Input Capture (4)	Traffic Signaling (1)		
				Scheduled Task/Job (6)		Indirect Command Execution		Peripheral Device Discovery		Screen Capture	Web Service (3)		
				Server Software Component (4)		Masquerading (7)		Permission Groups Discovery (3)		Video Capture			
				Traffic Signaling (1)		Modify Authentication Process (4)		Process Discovery					
				Valid Accounts (4)		Modify Cloud Compute Infrastructure (4)		Query Registry					
						Modify Registry		Remote System Discovery					
						Modify System Image (2)		Software Discovery (1)					
						Network Boundary Bridging (1)		System Information Discovery					
						Obfuscated Files or Information (6)		System Location Discovery (1)					
						Pre-OS Boot (5)		System Network Configuration Discovery (1)					
						Process Injection (11)		System Network Connections Discovery					
						Reflective Code Loading		System Owner/User Discovery					
						Rogue Domain Controller		System Service Discovery					
						Rootkit		System Time Discovery					
						Signed Binary Proxy Execution (13)		Virtualization/Sandbox Evasion (3)					
						Signed Script Proxy Execution (1)							
						Subvert Trust Controls (6)							
						Template Injection							
						Traffic Signaling (1)							
						Trusted Developer Utilities Proxy Execution (1)							
						Unused/Unsupported Cloud Regions							
						Use Alternate Authentication Material (4)							
						Valid Accounts (4)							
						Virtualization/Sandbox Evasion (3)							
						Weaken Encryption (2)							
						XSL Script Processing							

MITRE ATT&CK® stands for MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK). **The MITRE ATT&CK framework** is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's attack lifecycle and the platforms they are known to target. The tactics and techniques abstraction in the model provide a common taxonomy of individual adversary actions understood by both offensive and defensive sides of cybersecurity. It also provides an appropriate level of categorization for adversary action and specific ways of defending against it.

C.2m Attack Life Cycle: Cyber Kill Chain

MITRE ATT&CK



The MITRE ATT&CK matrix contains a set of techniques used by adversaries to accomplish a specific objective.

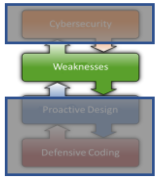
Those objectives are categorized as tactics in the ATT&CK Matrix. …

The objectives are presented linearly from the point of reconnaissance to the final goal of exfiltration or "impact".

The broadest version of ATT&CK for Enterprise, which includes Windows, macOS, Linux, PRE, Azure AD, Office 365, Google Workspace, SaaS, IaaS, Network, and Containers, categorizes 14 adversary tactics.

C.2n Attack Life Cycle: Cyber Kill Chain

MITRE ATT&CK



1.Reconnaissance: gathering information to plan future adversary operations, i.e., information about the target organization

2.Resource Development: establishing resources to support operations, i.e., setting up command and control infrastructure

3.Initial Access: trying to get into your network, i.e., spear phishing

4.Execution: trying the run malicious code, i.e., running a remote access tool …

5.Persistence: trying to maintain their foothold, i.e., changing configurations

6.Privilege Escalation: trying to gain higher-level permissions, i.e., leveraging a vulnerability to elevate access

7.Defense Evasion: trying to avoid being detected, i.e., using trusted processes to hide malware

8.Credential Access: stealing accounts names and passwords, i.e., keylogging

9.Discovery: trying to figure out your environment, i.e., exploring what they can control

10.Lateral Movement: moving through your environment, i.e., using legitimate credentials to pivot through multiple systems

11.Collection: gathering data of interest to the adversary goal, i.e., accessing data in cloud storage

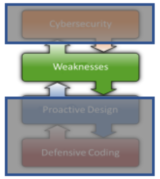
12.Command and Control: communicating with compromised systems to control them, i.e., mimicking normal web traffic to communicate with a victim network

13.Exfiltration: stealing data, i.e., transfer data to cloud account

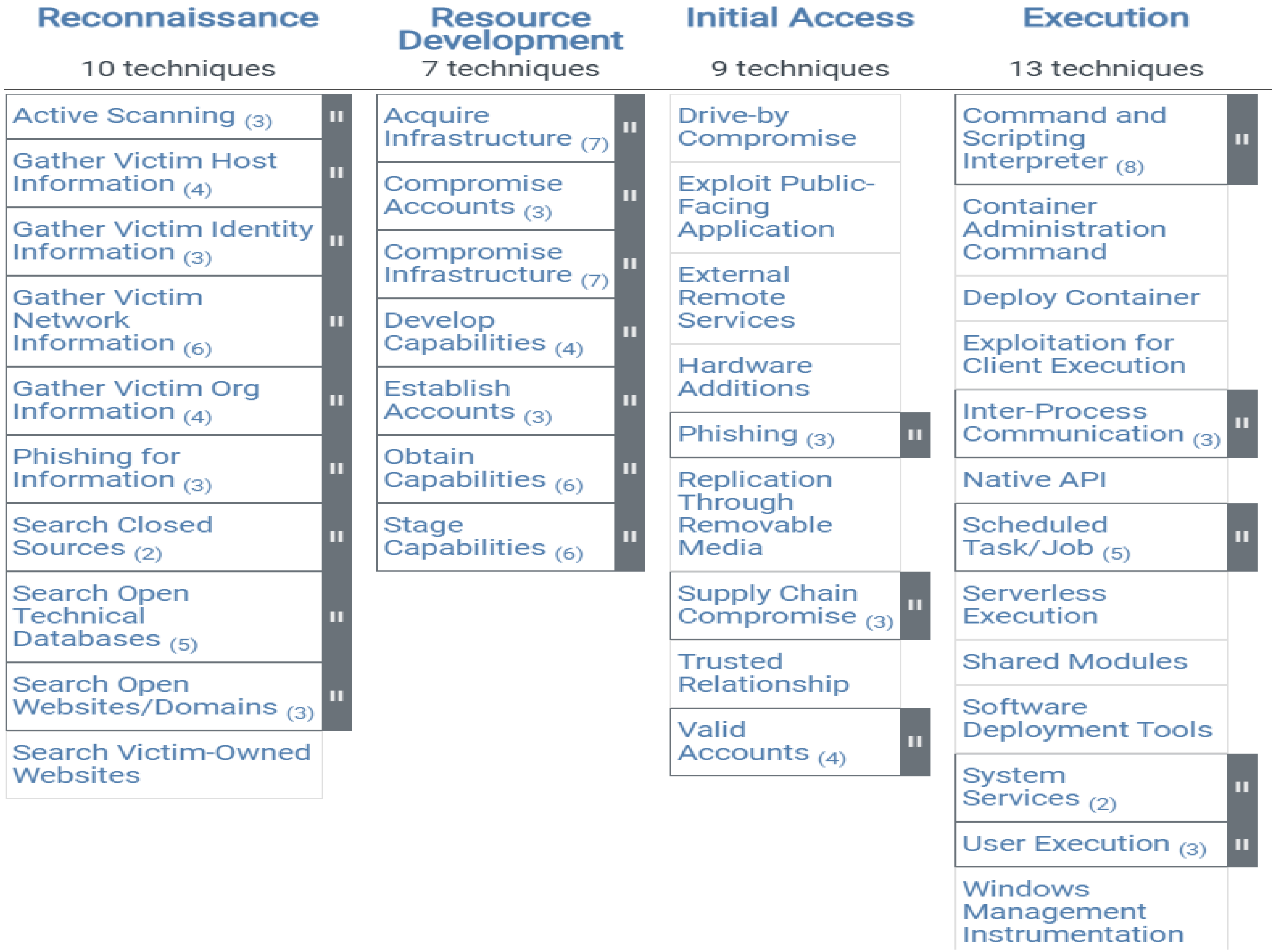
14.Impact: manipulate, interrupt, or destroy systems and data, i.e., encrypting data with ransomware

C.2n1 Attack Life Cycle: Cyber Kill Chain

MITRE ATT&CK



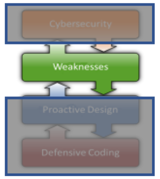
1. **Reconnaissance**: gathering information to plan future adversary operations, i.e., information about the target organization
2. **Resource Development**: establishing resources to support operations, i.e., setting up command and control infrastructure
3. **Initial Access**: trying to get into your network, i.e., spear phishing
4. **Execution**: trying the run malicious code, i.e., running a remote access tool



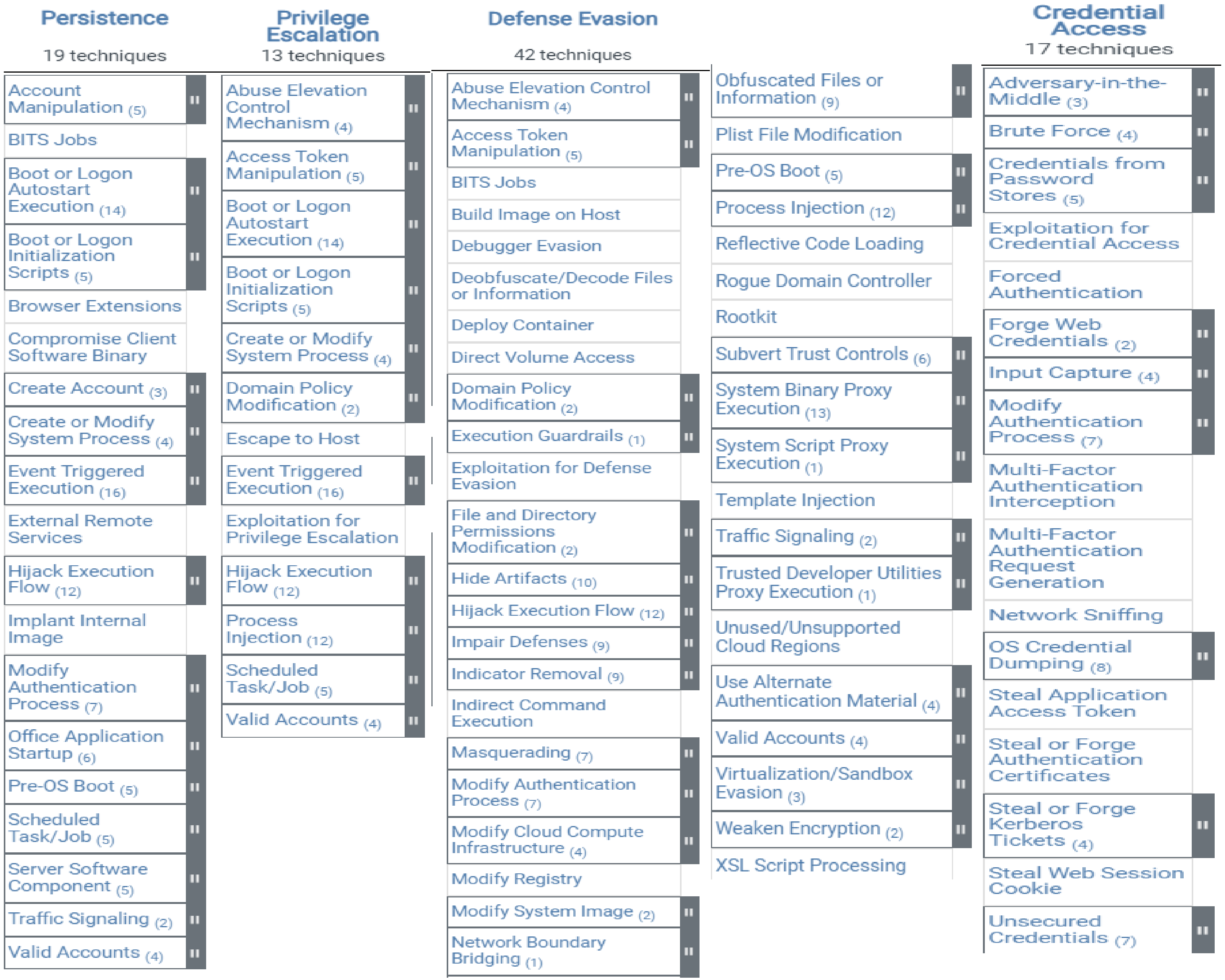
Reconnaissance	Resource Development	Initial Access	Execution
10 techniques	7 techniques	9 techniques	13 techniques
Active Scanning (3)	Acquire Infrastructure (7)	Drive-by Compromise	Command and Scripting Interpreter (8)
Gather Victim Host Information (4)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command
Gather Victim Identity Information (3)	Compromise Infrastructure (7)	External Remote Services	Deploy Container
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution
Gather Victim Org Information (4)	Establish Accounts (3)	Phishing (3)	Inter-Process Communication (3)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API
Search Closed Sources (2)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)
Search Open Technical Databases (5)		Trusted Relationship	Serverless Execution
Search Open Websites/Domains (3)		Valid Accounts (4)	Shared Modules
Search Victim-Owned Websites			Software Deployment Tools
			System Services (2)
			User Execution (3)
			Windows Management Instrumentation

C.2n2 Attack Life Cycle: Cyber Kill Chain

MITRE ATT&CK



5. **Persistence**: trying to maintain their foothold, i.e., changing configurations
6. **Privilege Escalation**: trying to gain higher-level permissions, i.e., leveraging a vulnerability to elevate access
7. **Defense Evasion**: trying to avoid being detected, i.e., using trusted processes to hide malware
8. **Credential Access**: stealing accounts names and passwords, i.e., keylogging



Persistence
19 techniques

Account Manipulation (5)
BITS Jobs
Boot or Logon Autostart Execution (14)
Boot or Logon Initialization Scripts (5)
Browser Extensions
Compromise Client Software Binary
Create Account (3)
Create or Modify System Process (4)
Event Triggered Execution (16)
External Remote Services
Hijack Execution Flow (12)
Implant Internal Image
Modify Authentication Process (7)
Office Application Startup (6)
Pre-OS Boot (5)
Scheduled Task/Job (5)
Server Software Component (5)
Traffic Signaling (2)
Valid Accounts (4)

Privilege Escalation
13 techniques

Abuse Elevation Control Mechanism (4)
Access Token Manipulation (5)
Boot or Logon Autostart Execution (14)
Boot or Logon Initialization Scripts (5)
Create or Modify System Process (4)
Domain Policy Modification (2)
Escape to Host
Event Triggered Execution (16)
Exploitation for Privilege Escalation
Hijack Execution Flow (12)
Process Injection (12)
Scheduled Task/Job (5)
Valid Accounts (4)

Defense Evasion
42 techniques

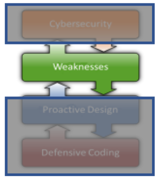
Abuse Elevation Control Mechanism (4)
Access Token Manipulation (5)
BITS Jobs
Build Image on Host
Debugger Evasion
Deobfuscate/Decode Files or Information
Deploy Container
Direct Volume Access
Domain Policy Modification (2)
Execution Guardrails (1)
Exploitation for Defense Evasion
File and Directory Permissions Modification (2)
Hide Artifacts (10)
Hijack Execution Flow (12)
Impair Defenses (9)
Indicator Removal (9)
Indirect Command Execution
Masquerading (7)
Modify Authentication Process (7)
Modify Cloud Compute Infrastructure (4)
Modify Registry
Modify System Image (2)
Network Boundary Bridging (1)
Obfuscated Files or Information (9)
Plist File Modification
Pre-OS Boot (5)
Process Injection (12)
Reflective Code Loading
Rogue Domain Controller
Rootkit
Subvert Trust Controls (6)
System Binary Proxy Execution (13)
System Script Proxy Execution (1)
Template Injection
Traffic Signaling (2)
Trusted Developer Utilities Proxy Execution (1)
Unused/Unsupported Cloud Regions
Use Alternate Authentication Material (4)
Valid Accounts (4)
Virtualization/Sandbox Evasion (3)
Weaken Encryption (2)
XSL Script Processing

Credential Access
17 techniques

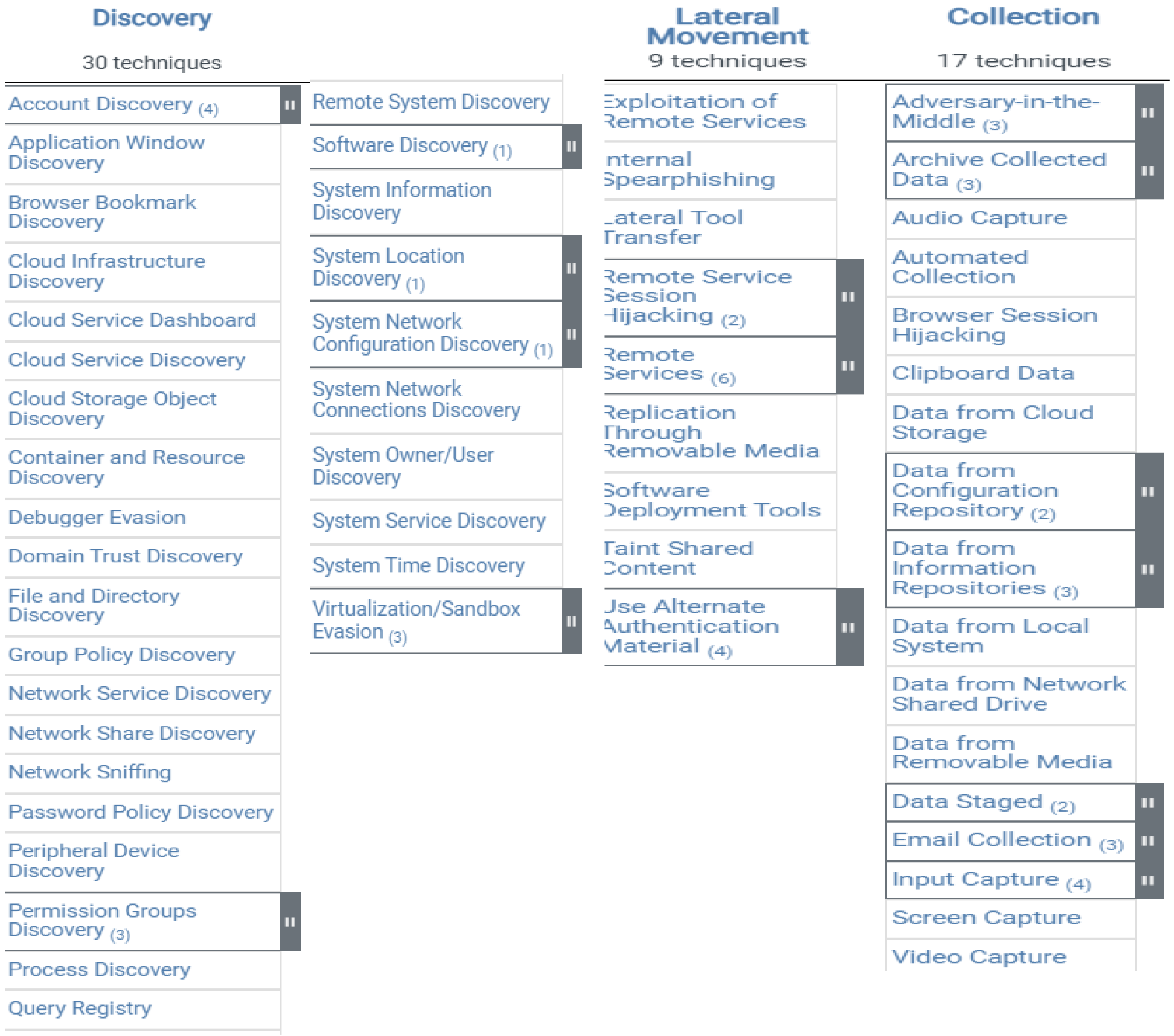
Adversary-in-the-Middle (3)
Brute Force (4)
Credentials from Password Stores (5)
Exploitation for Credential Access
Forced Authentication
Forge Web Credentials (2)
Input Capture (4)
Modify Authentication Process (7)
Multi-Factor Authentication Interception
Multi-Factor Authentication Request Generation
Network Sniffing
OS Credential Dumping (8)
Steal Application Access Token
Steal or Forge Authentication Certificates
Steal or Forge Kerberos Tickets (4)
Steal Web Session Cookie
Unsecured Credentials (7)

C.2n3 Attack Life Cycle: Cyber Kill Chain

MITRE ATT&CK



9. **Discovery**: trying to figure out your environment, i.e., exploring what they can control
10. **Lateral Movement**: moving through your environment, i.e., using legitimate credentials to pivot through multiple systems
11. **Collection**: gathering data of interest to the adversary goal, i.e., accessing data in cloud storage



Discovery

30 techniques

- Account Discovery (4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (1)
- System Information Discovery
- System Location Discovery (1)
- System Network Configuration Discovery (1)
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion (3)

Lateral Movement

9 techniques

- Exploitation of Remote Services
- nternal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (2)
- Remote Services (6)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (4)

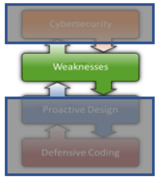
Collection

17 techniques

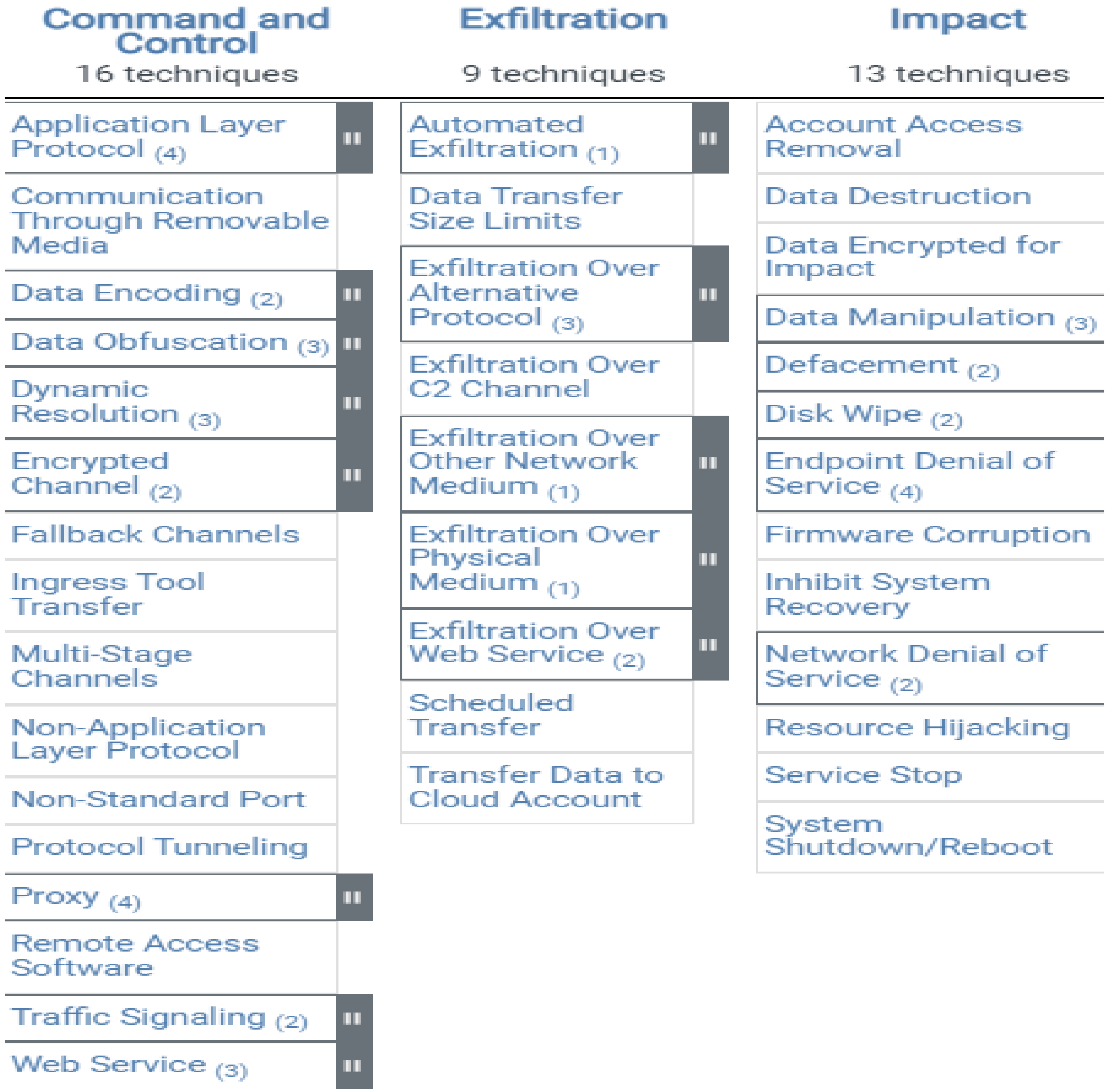
- Adversary-in-the-Middle (3)
- Archive Collected Data (3)
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage
- Data from Configuration Repository (2)
- Data from Information Repositories (3)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (2)
- Email Collection (3)
- Input Capture (4)
- Screen Capture
- Video Capture

C.2n4 Attack Life Cycle: Cyber Kill Chain

MITRE ATT&CK



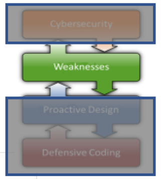
12. **Command and Control**: communicating with compromised systems to control them, i.e., mimicking normal web traffic to communicate with a victim network
13. **Exfiltration**: stealing data, i.e., transfer data to cloud account
14. **Impact**: manipulate, interrupt, or destroy systems and data, i.e., encrypting data with ransomware



Command and Control	Exfiltration	Impact
16 techniques	9 techniques	13 techniques
Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Non-Application Layer Protocol		Network Denial of Service (2)
Non-Standard Port		Resource Hijacking
Protocol Tunneling		Service Stop
Proxy (4)		System Shutdown/Reboot
Remote Access Software		
Traffic Signaling (2)		
Web Service (3)		

C.2o Attack Life Cycle: Cyber Kill Chain

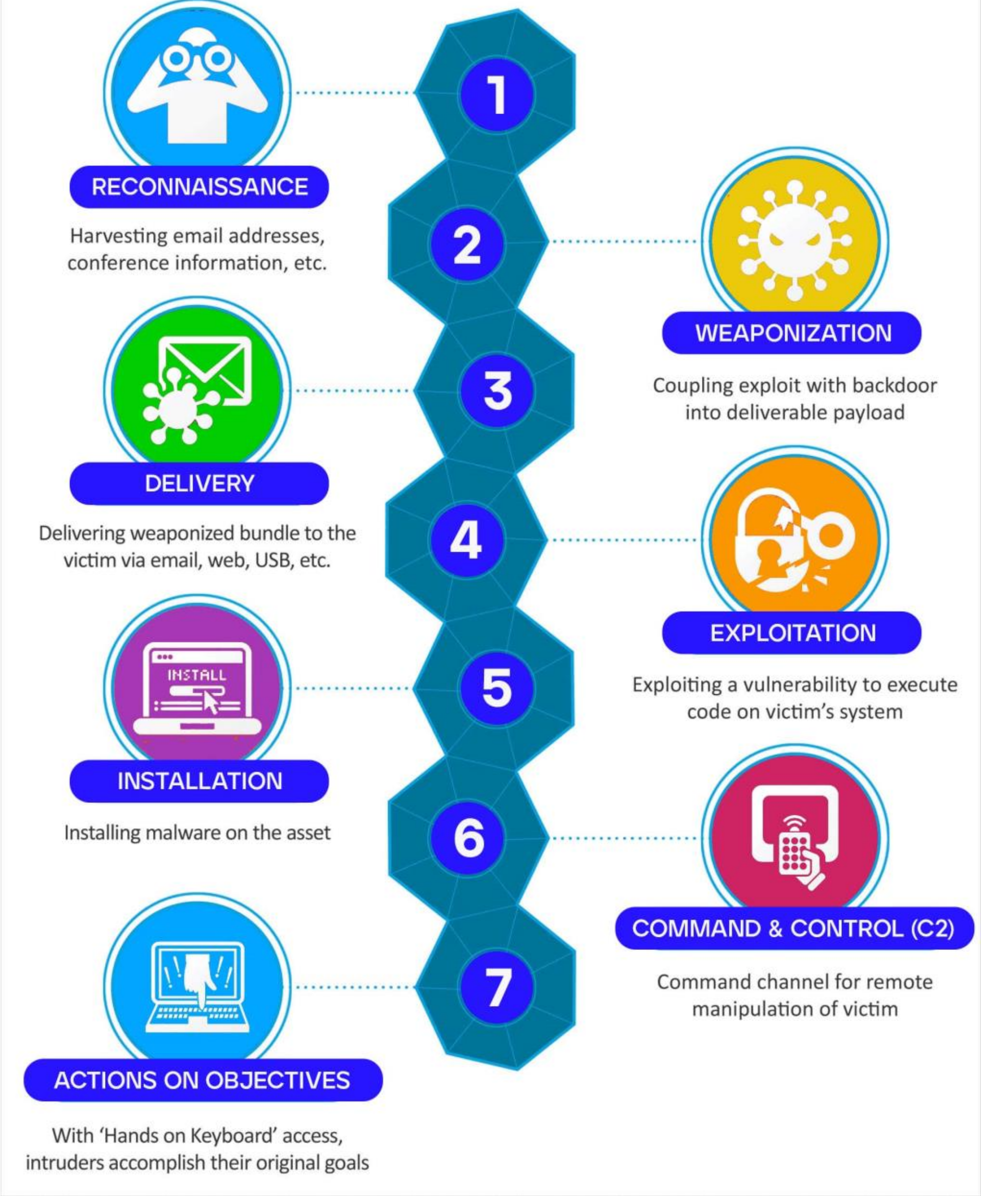
MITRE ATT&CK vs Cyber Kill Chain 1/3



The Lockheed Martin Cyber Kill Chain® is another well-known framework for understanding adversary behavior in a cyber-attack. The Kill Chain model contains the following stages, presented in sequence:

1. **Reconnaissance** – Harvests email addresses, conference information, etc.
2. **Weaponization** – Couples exploit with backdoor into deliverable payload.
3. **Delivery** – Delivers weaponized bundle to the victim via email, web, USB, etc.
4. **Exploitation** – Exploits a vulnerability to execute code on a victim's system.
5. **Installation** – Installs malware on the asset.
6. **Command & Control (C2)** – Includes command channel for remote manipulation.
7. **Actions on Objectives** – Using 'Hands on Keyboards' access, intruders accomplish their original goals.

Lockheed Martin gives more detail on their Cyber Kill Chain framework in this graphic. [3]



1 RECONNAISSANCE
Harvesting email addresses, conference information, etc.

2 WEAPONIZATION
Coupling exploit with backdoor into deliverable payload

3 DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.

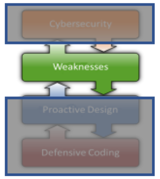
4 EXPLOITATION
Exploiting a vulnerability to execute code on victim's system

5 INSTALLATION
Installing malware on the asset

6 COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim

7 ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

C.2o Attack Life Cycle: Cyber Kill Chain



MITRE ATT&CK vs Cyber Kill Chain 2/3

Lockheed Martin Cyber Kill Chain®

1.Reconnaissance – Harvests email addresses, conference information, etc.

2.Weaponization – Couples exploit with backdoor into deliverable payload.

3.Delivery – Delivers weaponized bundle to the victim via email, web, USB, etc.

4.Exploitation – Exploits a vulnerability to execute code on a victim's system.

5.Installation – Installs malware on the asset.

6.Command & Control (C2) – Includes command channel for remote manipulation.

7.Actions on Objectives – Using 'Hands on Keyboards' access, intruders accomplish their original goals.

MITRE ATT&CK

1.Reconnaissance: gathering information to plan future adversary operations, i.e., information about the target organization

2.Resource Development: establishing resources to support operations, i.e., setting up command and control infrastructure

3.Initial Access: trying to get into your network, i.e., spear phishing

4.Execution: trying the run malicious code, i.e., running a remote access tool

5.Persistence: trying to maintain their foothold, i.e., changing configurations

6.Privilege Escalation: trying to gain higher-level permissions, i.e., leveraging a vulnerability to elevate access

7.Defense Evasion: trying to avoid being detected, i.e., using trusted processes to hide malware

8.Credential Access: stealing accounts names and passwords, i.e., keylogging

9.Discovery: trying to figure out your environment, i.e., exploring what they can control

10.Lateral Movement: moving through your environment, i.e., using legitimate credentials to pivot through multiple systems

11.Collection: gathering data of interest to the adversary goal, i.e., accessing data in cloud storage

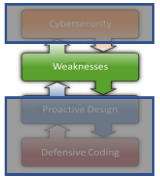
12.Command and Control: communicating with compromised systems to control them, i.e., mimicking normal web traffic to communicate with a victim network

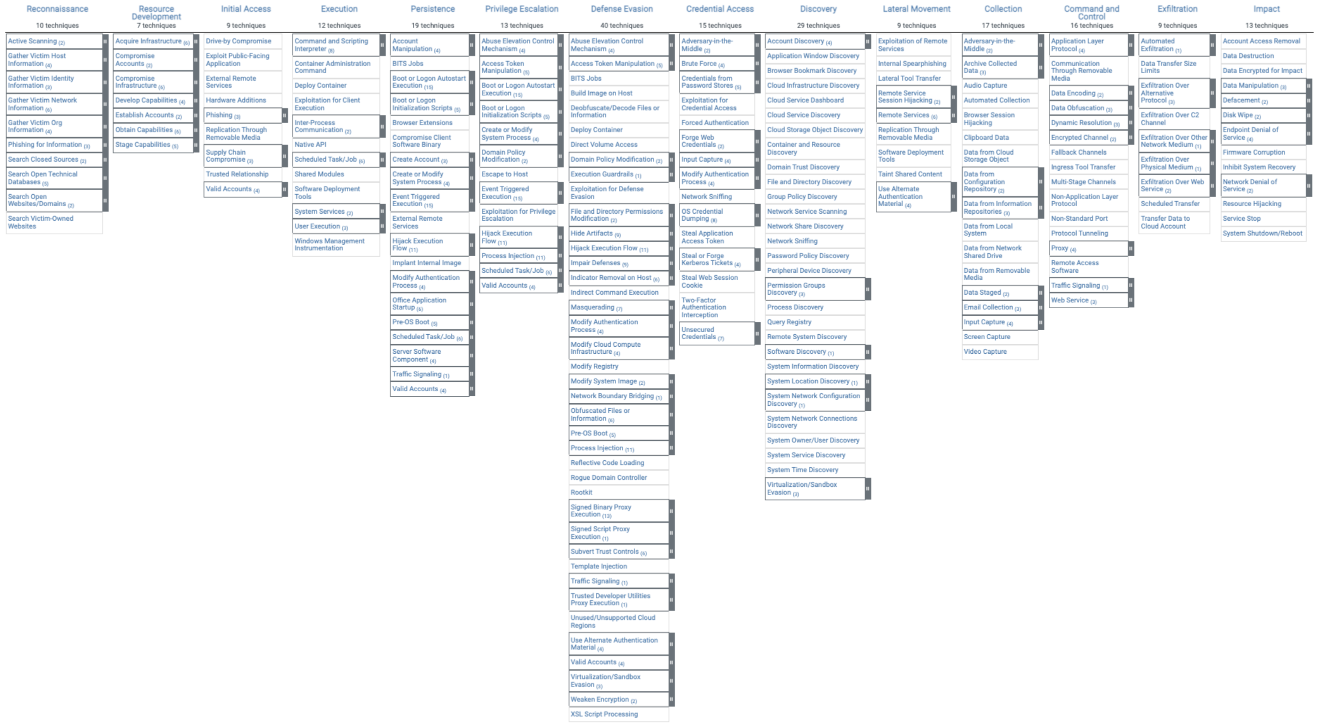
13.Exfiltration: stealing data, i.e., transfer data to cloud account

14.Impact: manipulate, interrupt, or destroy systems and data, i.e., encrypting data with ransomware

C.2p Attack Life Cycle: Cyber Kill Chain

MITRE ATT&CK vs Cyber Kill Chain 3/3





Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	40 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (15)	Boot or Logon Autostart Execution (15)	BITS Jobs
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (2)	Browser Extensions	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deploy Container
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (6)	Create Account (3)	Escape to Host	Direct Volume Access
Search Open Technical Databases (5)		Trusted Relationship	Shared Modules	Create or Modify System Process (4)	Event Triggered Execution (15)	Domain Policy Modification (2)
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment Tools	Event Triggered Execution (15)	Exploitation for Privilege Escalation	Execution Guardrails (1)
Search Victim-Owned Websites			System Services (2)	External Remote Services	Hijack Execution Flow (11)	Exploitation for Defense Evasion
			User Execution (3)	Hijack Execution Flow (11)	Process Injection (11)	File and Directory Permissions Modification (2)
			Windows Management Instrumentation	Implant Internal Image	Scheduled Task/Job (6)	Hide Artifacts (9)
				Modify Authentication Process (4)	Valid Accounts (4)	Hijack Execution Flow (11)
				Office Application Startup (6)		Impair Defenses (9)
				Pre-OS Boot (5)		Indicator Removal on Host (6)
				Scheduled Task/Job (6)		Indirect Command Execution
				Server Software Component (4)		Masquerading (7)
				Traffic Signaling (1)		Modify Authentication Process (4)
				Valid Accounts (4)		Modify Cloud Compute Infrastructure (4)
						Modify Registry
						Modify System Image (2)
						Network Boundary Bridging (1)
						Obfuscated Files or Information (6)
						Pre-OS Boot (5)
						Process Injection (11)
						Reflective Code Loading
						Rogue Domain Controller
						Rootkit
						Signed Binary Proxy Execution (13)
						Signed Script Proxy Execution (1)
						Subvert Trust Controls (6)
						Template Injection
						Traffic Signaling (1)
						Trusted Developer Utilities Proxy Execution (1)
						Unused/Unsupported Cloud Regions
						Use Alternate Authentication Material (4)
						Valid Accounts (4)
						Virtualization/Sandbox Evasion (3)
						Weaken Encryption (2)
						XSL Script Processing

Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
15 techniques	29 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Adversary-in-the-Middle (2)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (2)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Credentials from Password Stores (5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Forced Authentication	Cloud Service Dashboard	Remote Services (6)	Browser Session Hijacking	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage Object	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Modify Authentication Process (4)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Network Sniffing	Domain Trust Discovery	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
OS Credential Dumping (8)	File and Directory Discovery		Data from Local System	Non-Application Layer Protocol		Network Denial of Service (2)
Steal Application Access Token	Group Policy Discovery		Data from Network Shared Drive	Non-Standard Port		Resource Hijacking
Steal or Forge Kerberos Tickets (4)	Network Service Scanning		Data from Removable Media	Protocol Tunneling		Service Stop
Steal Web Session Cookie	Network Share Discovery		Data Staged (2)	Proxy (4)		System Shutdown/Reboot
Two-Factor Authentication Interception	Network Sniffing		Email Collection (3)	Remote Access Software		
Unsecured Credentials (7)	Password Policy Discovery		Input Capture (4)	Traffic Signaling (1)		
	Peripheral Device Discovery		Screen Capture	Web Service (3)		
	Permission Groups Discovery (3)		Video Capture			
	Process Discovery					
	Query Registry					
	Remote System Discovery					
	Software Discovery (1)					
	System Information Discovery					
	System Location Discovery (1)					
	System Network Configuration Discovery (1)					
	System Network Connections Discovery					
	System Owner/User Discovery					
	System Service Discovery					
	System Time Discovery					
	Virtualization/Sandbox Evasion (3)					

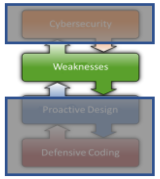
There are two primary differences between MITRE ATT&CK and Cyber Kill Chain.

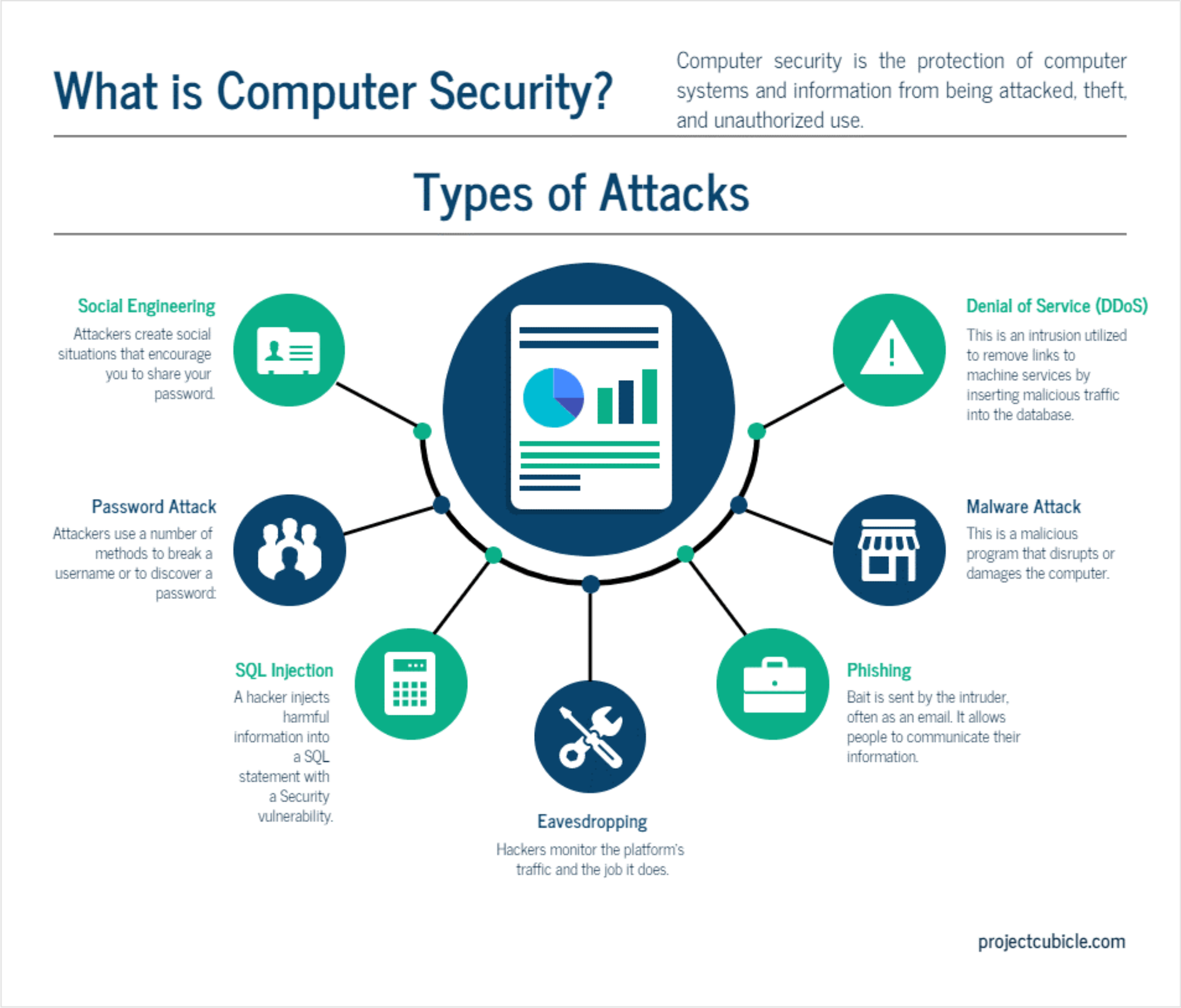
1. First, the MITRE ATT&CK framework goes into significantly more depth on how each stage is conducted through ATT&CK techniques and sub-techniques. MITRE ATT&CK is regularly updated with industry input to keep up with the latest techniques so defenders update their own practices and attack modeling regularly.

2.Second, the Cyber Kill Chain does not factor in the different tactics and techniques of a cloud-native attack, as discussed above. The Cyber Kill Chain framework assumes that an adversary will deliver a payload, such as malware, to the target environment; a method which is much less relevant in the cloud.

C.2r Attack Life Cycle: Cyber Kill Chain

Types of Attacks





What is Computer Security?

Computer security is the protection of computer systems and information from being attacked, theft, and unauthorized use.

Types of Attacks

Social Engineering
Attackers create social situations that encourage you to share your password.

Password Attack
Attackers use a number of methods to break a username or to discover a password.

SQL Injection
A hacker injects harmful information into a SQL statement with a Security vulnerability.

Eavesdropping
Hackers monitor the platform's traffic and the job it does.

Phishing
Bait is sent by the intruder, often as an email. It allows people to communicate their information.

Malware Attack
This is a malicious program that disrupts or damages the computer.

Denial of Service (DDoS)
This is an intrusion utilized to remove links to machine services by inserting malicious traffic into the database.

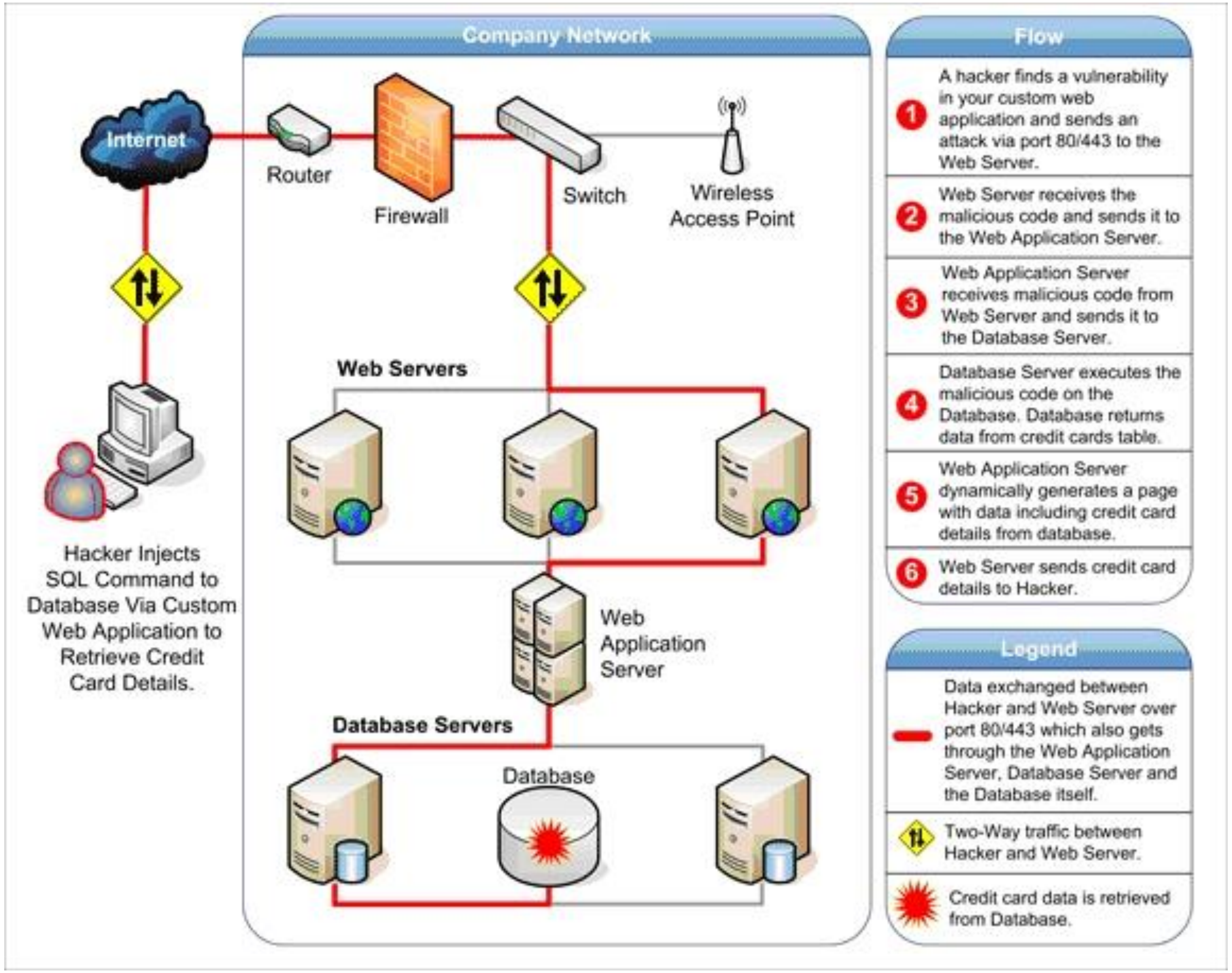
projectcubicle.com

…

Techniques to avoid being identified by End-Point protection systems

C.2s Attack Life Cycle: Cyber Kill Chain

Web Application Attack



Flow

1. A hacker finds a vulnerability in your custom web application and sends an attack via port 80/443 to the Web Server.
2. Web Server receives the malicious code and sends it to the Web Application Server.
3. Web Application Server receives malicious code from Web Server and sends it to the Database Server.
4. Database Server executes the malicious code on the Database. Database returns data from credit cards table.
5. Web Application Server dynamically generates a page with data including credit card details from database.
6. Web Server sends credit card details to Hacker.

Legend

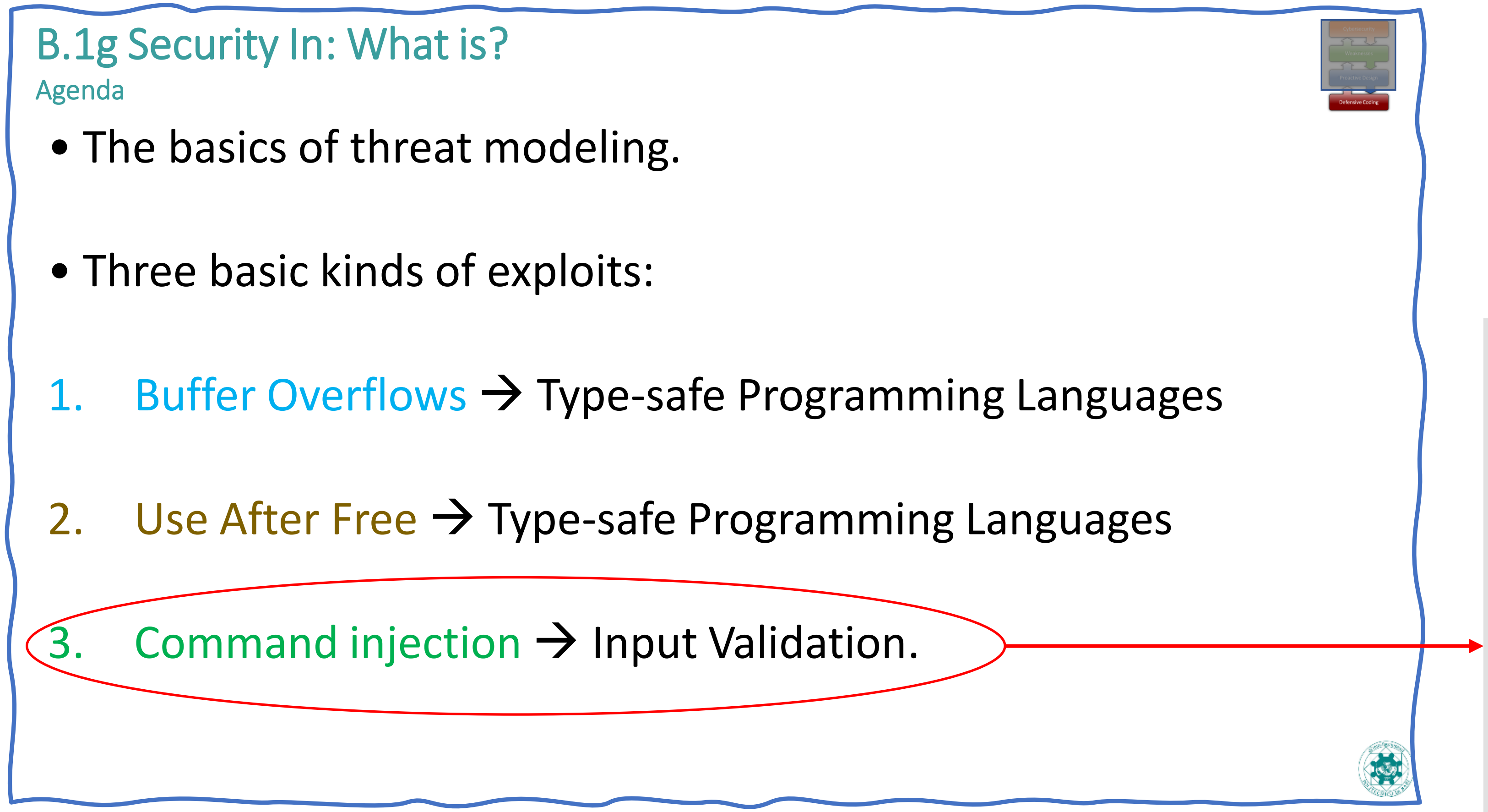
- 🟥 Data exchanged between Hacker and Web Server over port 80/443 which also gets through the Web Application Server, Database Server and the Database itself.
- ⇅ Two-Way traffic between Hacker and Web Server.
- ✹ Credit card data is retrieved from Database.

What Is a Web Application Attack and how to Defend Against It:

https://www.acunetix.com/websitesecurity/web-application-attack/

C.2t1 Attack Life Cycle: Cyber Kill Chain

Web Application Attack



B.1g Security In: What is?

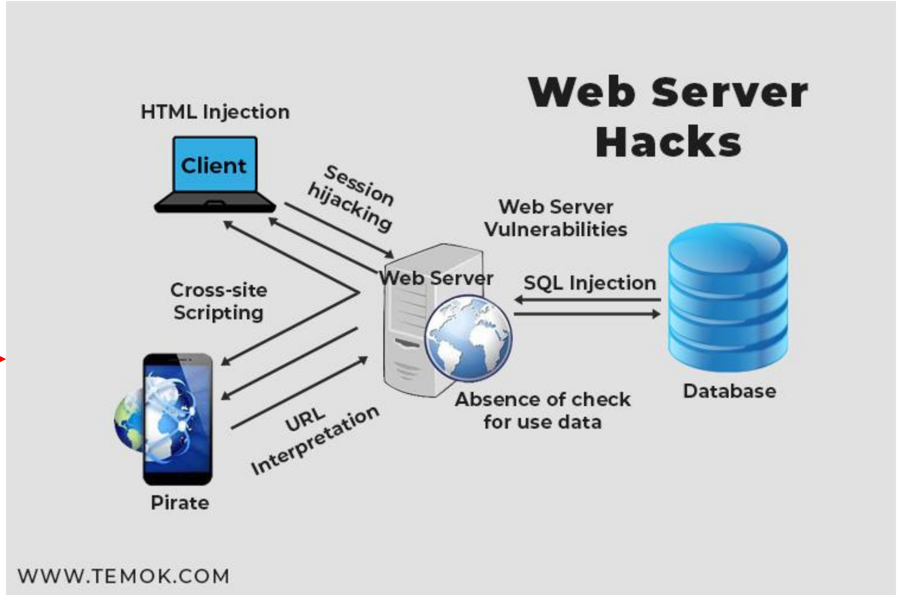
Agenda

- The basics of threat modeling.
- Three basic kinds of exploits:

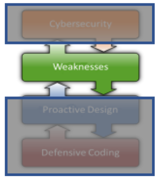
1. Buffer Overflows → Type-safe Programming Languages
2. Use After Free → Type-safe Programming Languages
3. Command injection → Input Validation.

If the online developers don’t adopt secure coding practices while developing web applications, it may give attackers the prospect to exploit vulnerabilities and compromise web applications and web server security.

Even if web servers are **configured securely** or are secured using network security measures like firewalls, a **poorly coded web application** deployed on the online server may provide a path to an attacker to compromise the online server’s security.



WWW.TEMOK.COM



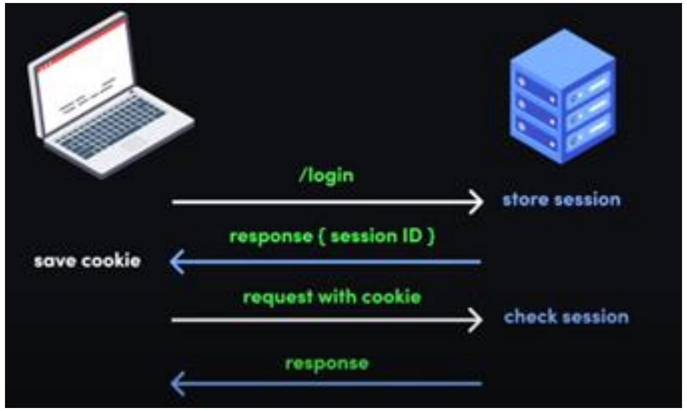
C.2t2 Attack Life Cycle: Cyber Kill Chain

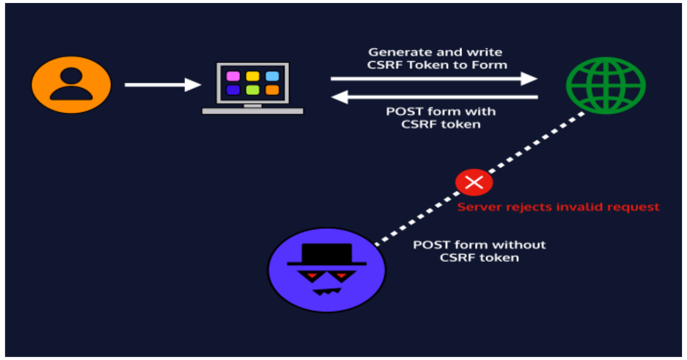
Web Application Attack

An attacker can perform different types of attacks on vulnerable web applications to breach web server security.

- **Unvalidated Input and File Injection Attacks:** Unvalidated input and file injection attacks are performed by supplying an unvalidated input or by injecting files into an internet application.
- **Parameter/Form Tampering:** during this sort of tampering attack, the attacker manipulates the parameters exchanged between client and server so as to switch application data, like user credentials and permissions, price and quantity of products, and so on.
- **Command Injection Attacks:** during this sort of attack, a hacker alters the content of the online page by using html code and by identifying the form fields that lack valid constraints.
- **SQL Injection Attacks:** SQL injection t exploits the safety vulnerability of a database for attacks. The attacker injects malicious code into the strings, later passed on to the SQL Server for execution.
- **Cookie Tampering:** Cookie tampering attacks occur when sending a cookie from the client-side to the server. differing types of toots help in modifying persistent and non-persistent cookies.
- **Session Hijacking:** Session hijacking is an attack during which the attacker exploits, steals,predicts, and negotiates the important valid web session's control mechanism to access the authenticated parts of an internet application.
- **Cross-Ste Request Forgery (CSRF) Attack:** An attacker exploits the trust of an authenticated user to pass malicious code or commands to the online server
- **Cross-Site Scripting (XSS) Attacks:** during this method, an attacker injects HTML tags or scripts into a target website.
  Buffer Overflow Attacks: the planning of most web applications helps them in sustaining some amount of knowledge. If that amount exceeds the storage space available, the appliance may crash or may exhibit some other vulnerable behaviour. The attacker uses this advantage and floods the appliance with too much data, which successively causes a buffer overflow attack,

```
"SELECT *
FROM users
WHERE login=$name
AND password = $pwd"
```




Generate and write CSRF Token to Form
POST form with CSRF token
Server rejects invalid request
POST form without CSRF token

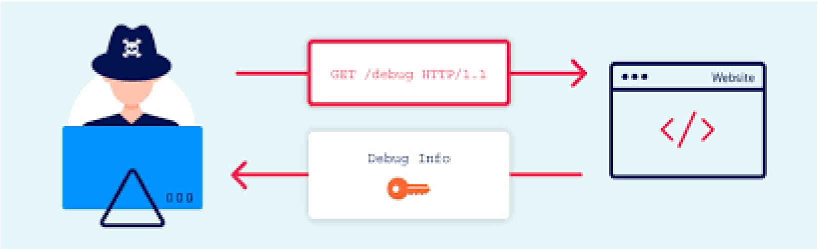
C.2t3 Attack Life Cycle: Cyber Kill Chain

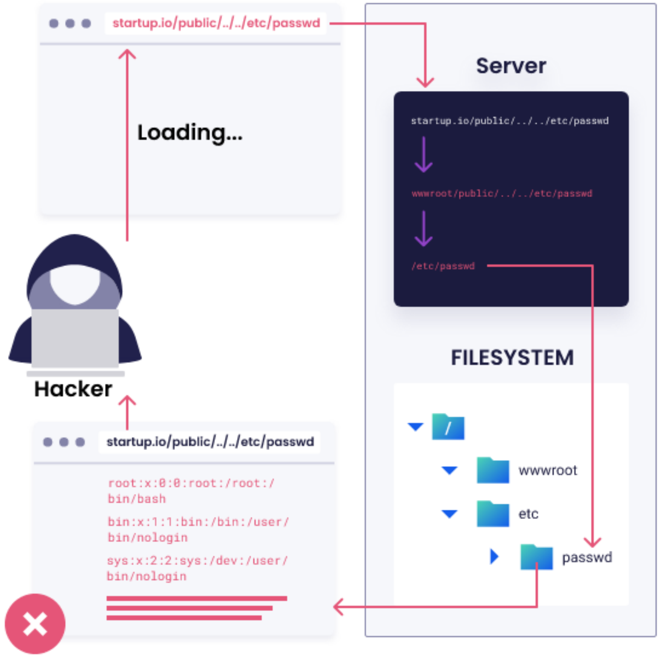
Web Application Attack

An attacker can perform different types of attacks on vulnerable web applications to breach web server security.

Secure Configuration

- **ASCII text file Disclosure:** source code disclosure may be a results of typographical errors in scripts or due to misconfiguration, like failing to grant executable permissions to a script or directory. This disclosure can sometimes allow the attackers to realize sensitive information about database credentials and secret keys and compromise the online servers.



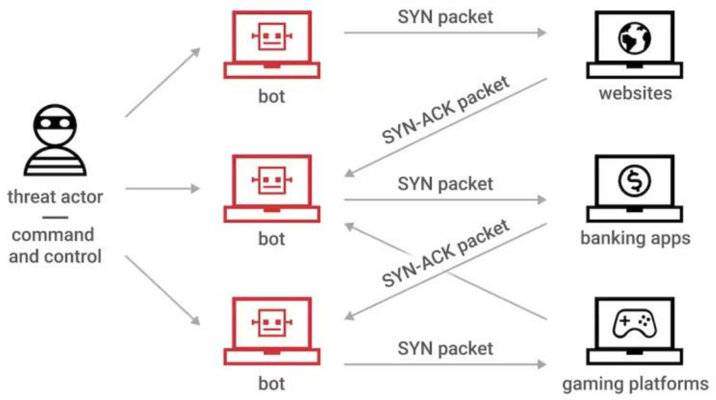

startup.io/public/../../etc/passwd
Loading...
Hacker
Server
startup.io/public/../../etc/passwd
wwwroot/public/../../etc/passwd
/etc/passwd
FILESYSTEM
/
wwwroot
etc
passwd
startup.io/public/../../etc/passwd

```
root:x:0:0:root:/root:/
bin/bash
bin:x:1:1:bin:/bin:/user/
bin/nologin
sys:x:2:2:sys:/dev:/user/
bin/nologin
```

- **Directory Traversal:** Directory traversal is that the exploitation of HTTP through which attackers can access restricted directories and execute commands outside of the online server’s root directory by manipulating a URL.

Security Architecture

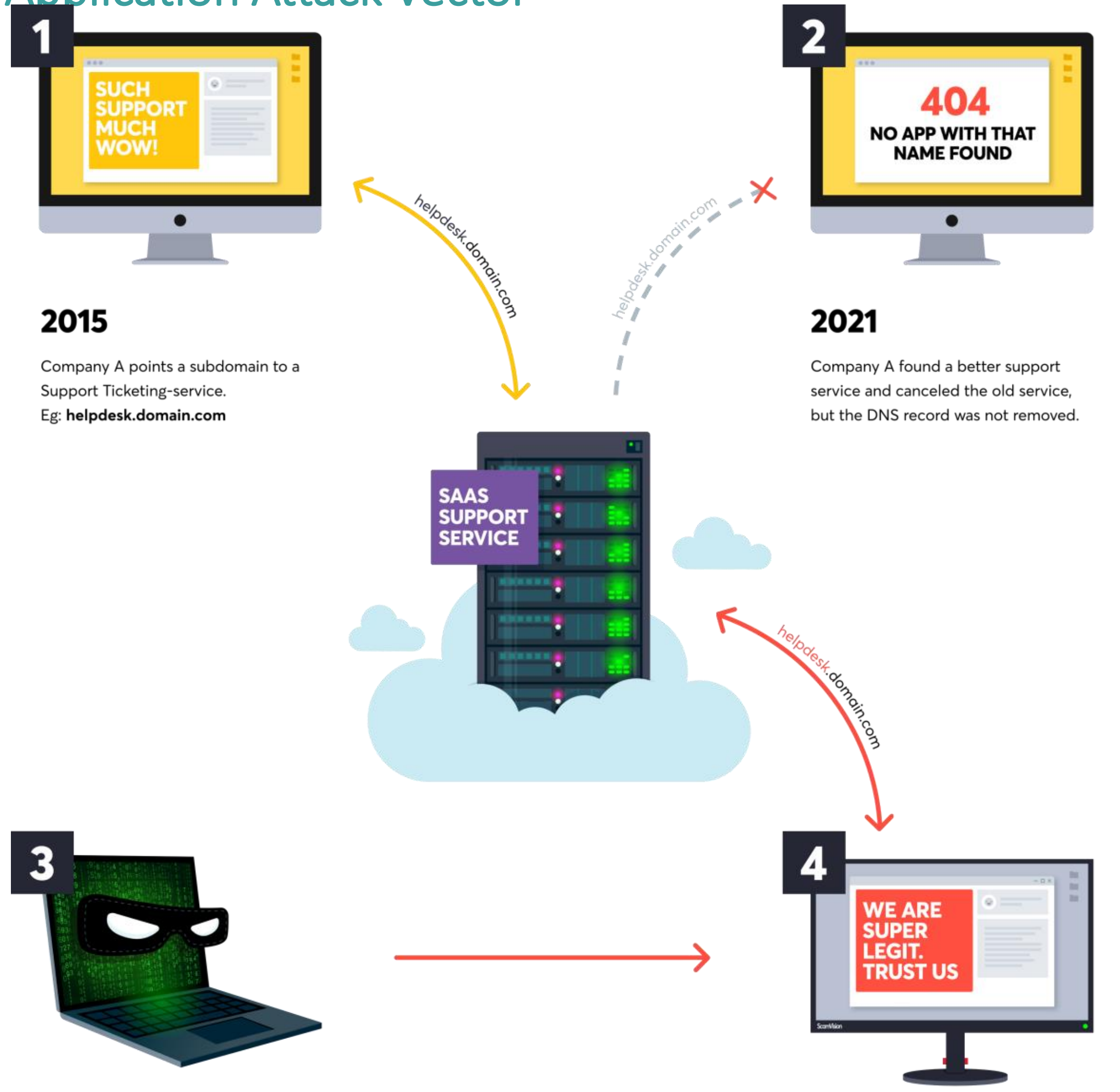
- **Denial-of.Service (DoS) Attack:** A DOS attack is meant to terminate the operations of a website or a server and make it unavailable for access by intended users.



What is a DDoS attack? – Protocol

C.2u Attack Life Cycle: Cyber Kill Chain

Web Application Attack Vector



2015

Company A points a subdomain to a Support Ticketing-service.
Eg: **helpdesk.domain.com**

2021

Company A found a better support service and canceled the old service, but the DNS record was not removed.

An attacker sees that Company A points a domain to a service no longer in use. They sign up for the service and claim the domain without verification.

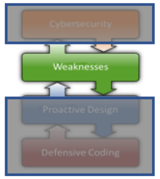
Attacker builds a convincing clone of Company A's support site and uses it to phish users and steal sensitive cookie data.

…

https://detectify.com/attack-vector

C.2v Attack Life Cycle: Cyber Kill Chain

Web Attack Using the Browser



Three web attack vectors seem to be responsible for the majority of computer attacks that involve a web browser:

•The attack can incorporate an element of social engineering to persuade the victim to take an action that compromises security. For instance, the victim can supply data to a phishing site or install a program that will turn out to be malicious.

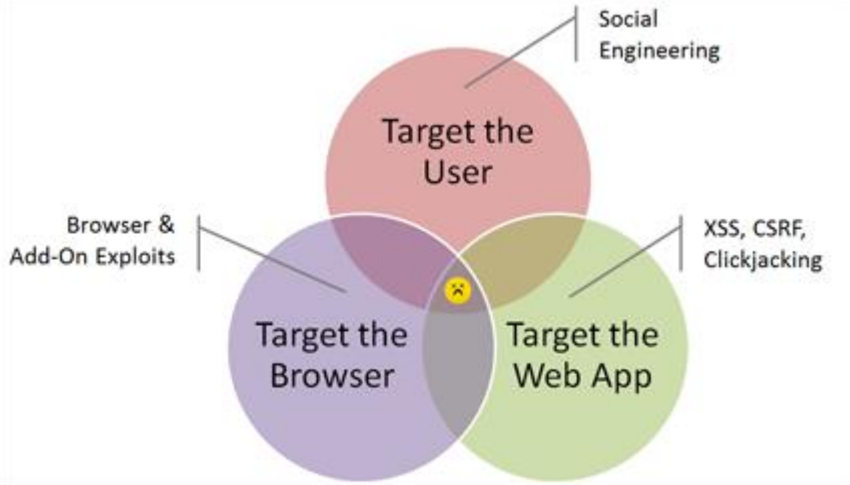
•The attacker can use the browser as a gateway for attacking web applications via techniques such as cross-site scripting (XSS), Cross-Site Request Forgery (CSRF) and Clickjacking.

•The attacker can exploit a vulnerability in the web browser or in local software that the browser can invoke. Such client-side exploits have targeted browser add-ons such as Flash, Adobe Reader and Java Runtime Environment (JRE).

Most attacks include one or two of the three techniques. For instance, Koobface worm targets the user (social engineering to click links) and the web application (hijacking social networking site sessions).

The following series of posts explores these three web browser attack vectors in greater detail, discussing how enterprises can protect themselves against such attacks:

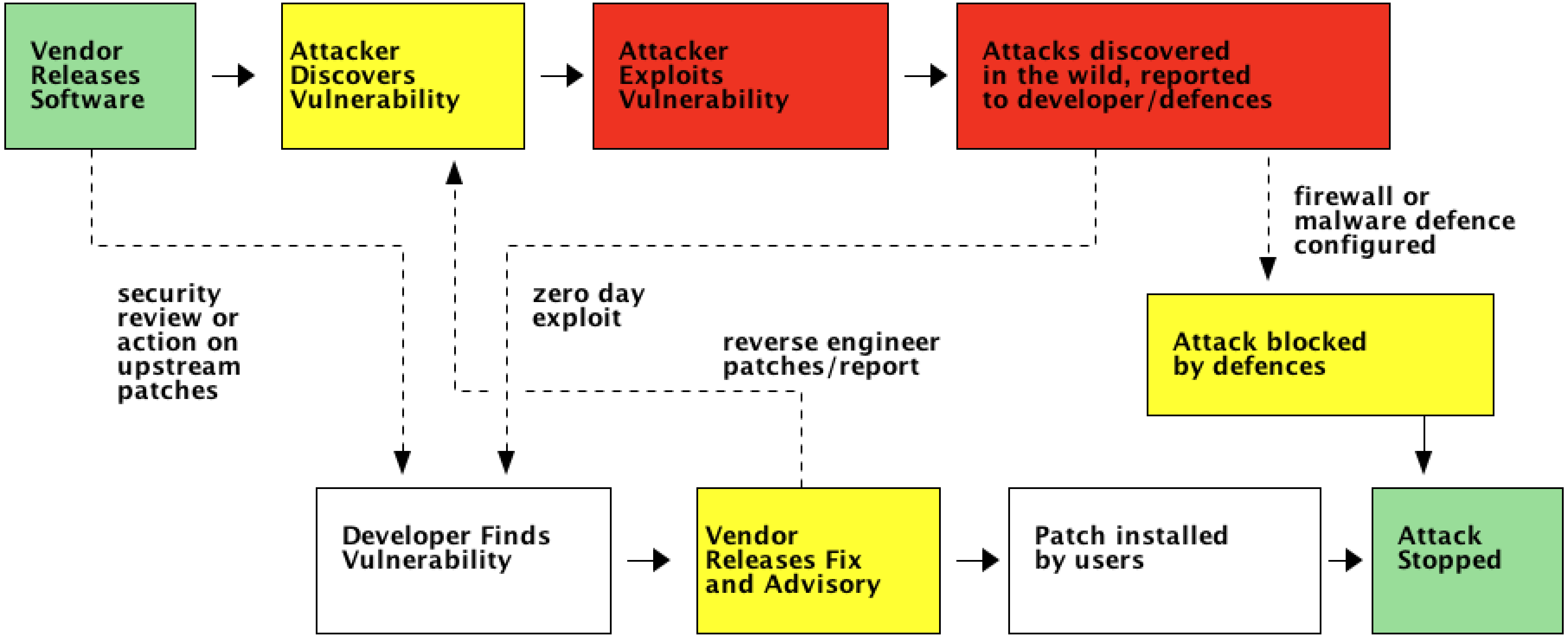
- Mitigating Attacks on the User of the Web Browser
- Mitigating Attacks on Web Applications Through the Browser
- Mitigating Attacks on the Web Browser and Add-Ons



https://zeltser.com/web-browser-attack-vectors/

C.3 Attackers & Vulnerabilities

Attackers vs Vendors



Vendor Releases Software

Attacker Discovers Vulnerability

Attacker Exploits Vulnerability

Attacks discovered in the wild, reported to developer/defences

security review or action on upstream patches

zero day exploit

reverse engineer patches/report

firewall or malware defence configured

Attack blocked by defences

Developer Finds Vulnerability

Vendor Releases Fix and Advisory

Patch installed by users

Attack Stopped

Advisories == Security Bullettin

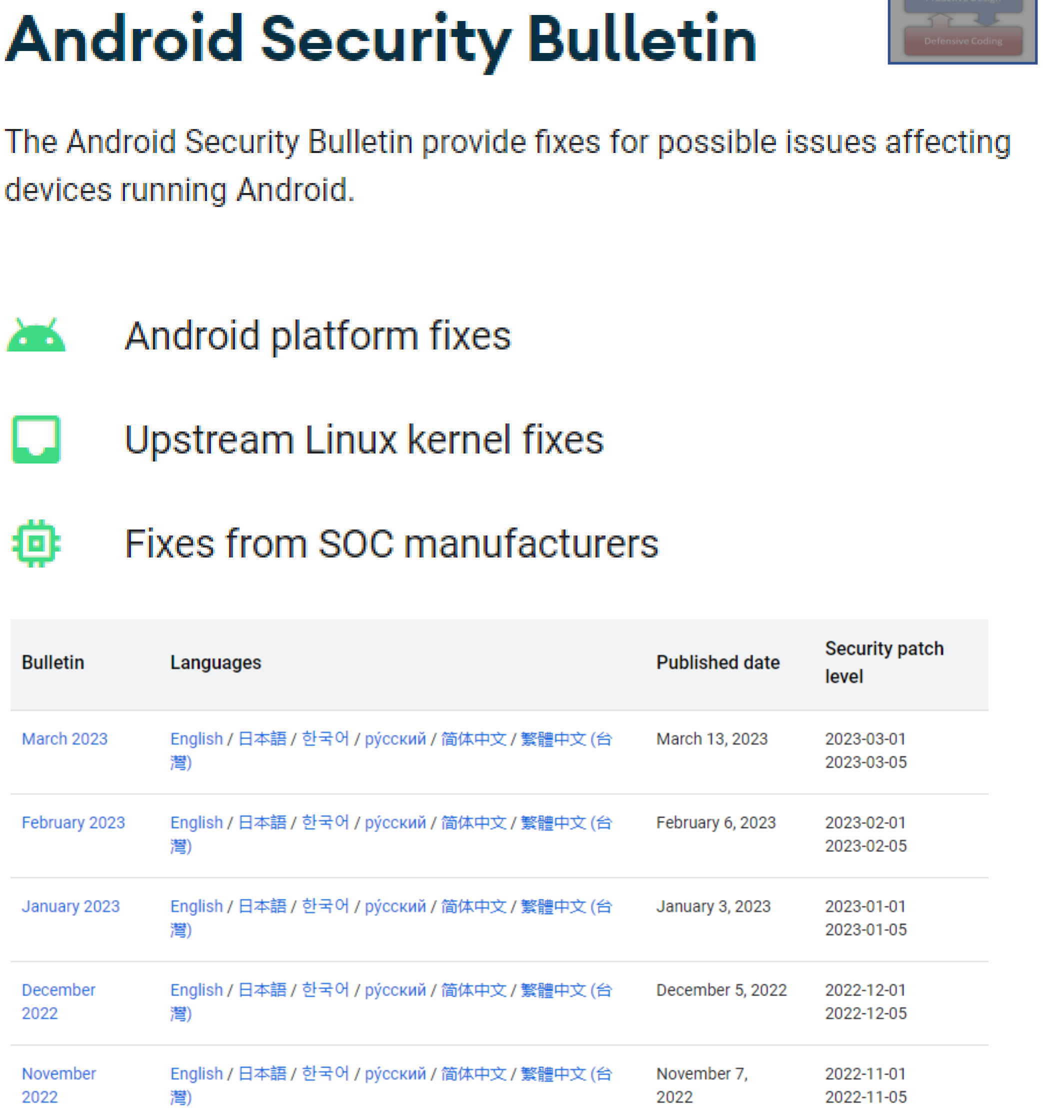
C.3a Attackers & Vulnerabilities

Security Bullettin

Security advisories (aka bulletins) are issued by software vendors

- ▶ public feeds, also private at earlier stages
- ▶ advance notification to high-value customers, security companies
- ▶ maybe before patches are available
- ▶ (Q. is that a good idea?)
- ▶ public advisory usually when update available

Various people (sys admins, downstream software devs, users...) should monitor and act on advisories.



Android Security Bulletin

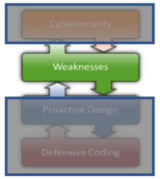
The Android Security Bulletin provide fixes for possible issues affecting devices running Android.

- Android platform fixes
- Upstream Linux kernel fixes
- Fixes from SOC manufacturers

Bulletin	Languages	Published date	Security patch level
March 2023	English / 日本語 / 한국어 / русский / 简体中文 / 繁體中文 (台灣)	March 13, 2023	2023-03-01 2023-03-05
February 2023	English / 日本語 / 한국어 / русский / 简体中文 / 繁體中文 (台灣)	February 6, 2023	2023-02-01 2023-02-05
January 2023	English / 日本語 / 한국어 / русский / 简体中文 / 繁體中文 (台灣)	January 3, 2023	2023-01-01 2023-01-05
December 2022	English / 日本語 / 한국어 / русский / 简体中文 / 繁體中文 (台灣)	December 5, 2022	2022-12-01 2022-12-05
November 2022	English / 日本語 / 한국어 / русский / 简体中文 / 繁體中文 (台灣)	November 7, 2022	2022-11-01 2022-11-05

C.3b Attackers & Vulnerabilities

Vulnerability Disclosure

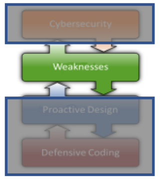


The process by which the analysis of these vulnerabilities is shared with third parties is the subject of much debate, and is referred to as the researcher's disclosure policy.

1. **Coordinated Disclosure**: policy under which researchers agree to report vulnerabilities to a coordinating authority, which then reports it to the vendor, tracks fixes and mitigations, and coordinates the disclosure of information with stakeholders including the public. The premise of coordinated disclosure is typically that nobody should be informed about a vulnerability until the software vendor says it is time, or, at max 30 days after the reporting to the coordinating authority.
2. **Full Disclosure**: policy of publishing information on vulnerabilities without restriction as early as possible, making the information accessible to the general public without restriction. In general, proponents of full disclosure believe that the benefits of freely available vulnerability research outweigh the risks, whereas opponents prefer to limit the distribution.
3. **Non Disclosure**: policy of not sharing at all the vulnerability information, or should only be shared under non-disclosure agreement (either contractually or informally)

C.3c Attackers & Vulnerabilities

The ZDI: Zero Day Initiative



https://www.zerodayinitiative.com/about/

started by TippingPoint, a network security company

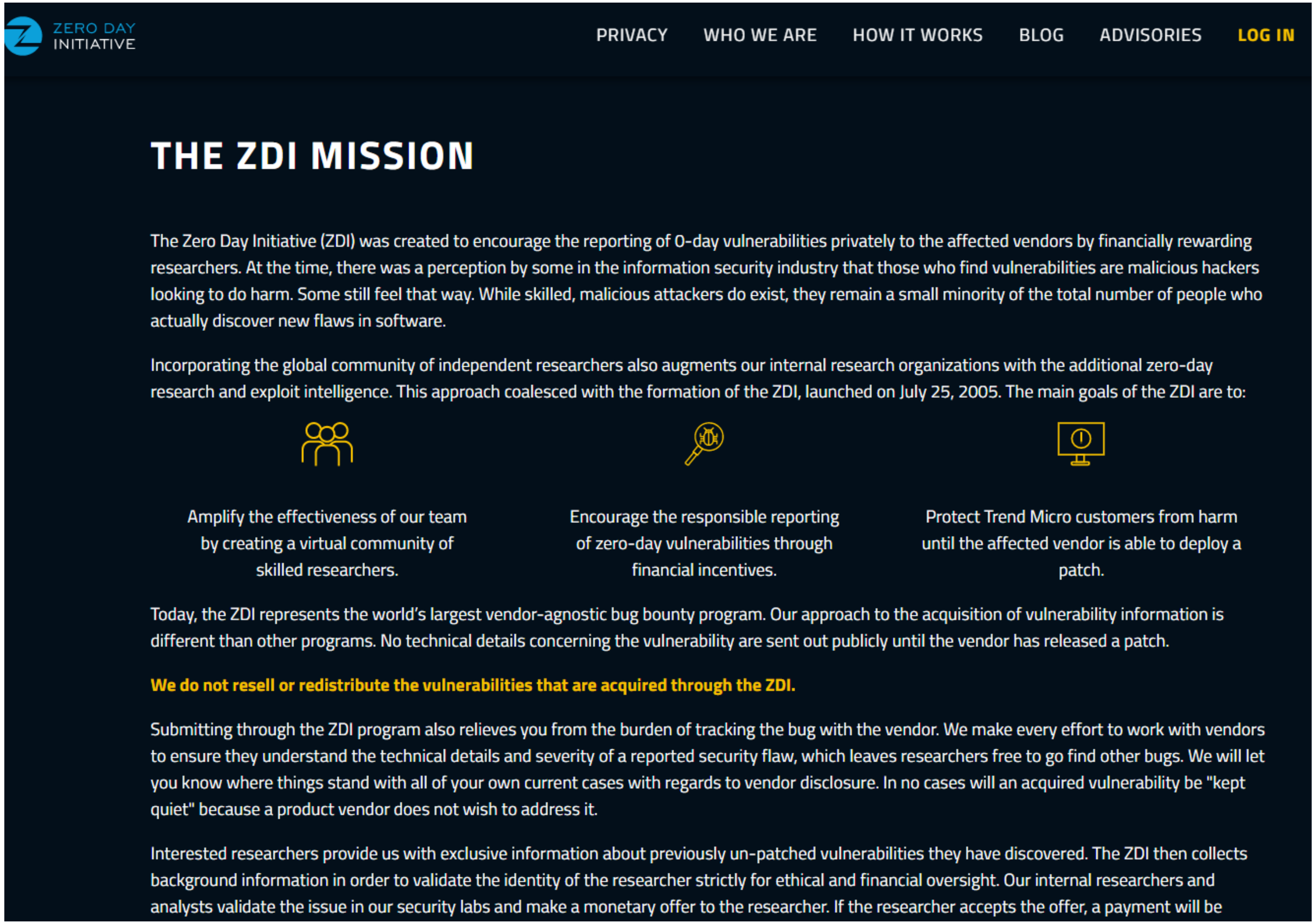
Idea of "buying vulnerability" by crowd-souring discovery

Incentive programme rewarding participants

▶ $ reward, bonuses like DEFCON attendance

▶ advantages: independence, wider knowledge

▶ and presumably cheaper than direct employment



THE ZDI MISSION

The Zero Day Initiative (ZDI) was created to encourage the reporting of 0-day vulnerabilities privately to the affected vendors by financially rewarding researchers. At the time, there was a perception by some in the information security industry that those who find vulnerabilities are malicious hackers looking to do harm. Some still feel that way. While skilled, malicious attackers do exist, they remain a small minority of the total number of people who actually discover new flaws in software.

Incorporating the global community of independent researchers also augments our internal research organizations with the additional zero-day research and exploit intelligence. This approach coalesced with the formation of the ZDI, launched on July 25, 2005. The main goals of the ZDI are to:

Amplify the effectiveness of our team by creating a virtual community of skilled researchers.

Encourage the responsible reporting of zero-day vulnerabilities through financial incentives.

Protect Trend Micro customers from harm until the affected vendor is able to deploy a patch.

Today, the ZDI represents the world's largest vendor-agnostic bug bounty program. Our approach to the acquisition of vulnerability information is different than other programs. No technical details concerning the vulnerability are sent out publicly until the vendor has released a patch.

We do not resell or redistribute the vulnerabilities that are acquired through the ZDI.

Submitting through the ZDI program also relieves you from the burden of tracking the bug with the vendor. We make every effort to work with vendors to ensure they understand the technical details and severity of a reported security flaw, which leaves researchers free to go find other bugs. We will let you know where things stand with all of your own current cases with regards to vendor disclosure. In no cases will an acquired vulnerability be "kept quiet" because a product vendor does not wish to address it.

Interested researchers provide us with exclusive information about previously un-patched vulnerabilities they have discovered. The ZDI then collects background information in order to validate the identity of the researcher strictly for ethical and financial oversight. Our internal researchers and analysts validate the issue in our security labs and make a monetary offer to the researcher. If the researcher accepts the offer, a payment will be