SOFTWARE DEFINED VIRTUAL NETWORKING SECURITY

CHAPTER 11 INTELLIGENT SOFTWARE DEFINED SECURITY

Dijiang Huang, Ankur Chowdhary, and Sandeep Pisharody

OUTLINE

- Intelligence in Network Security
- Application of Machine Learning (ML) and AI in Security
- Advanced Persistent Threats
- Problems in Application of Intelligence in Cybersecurity

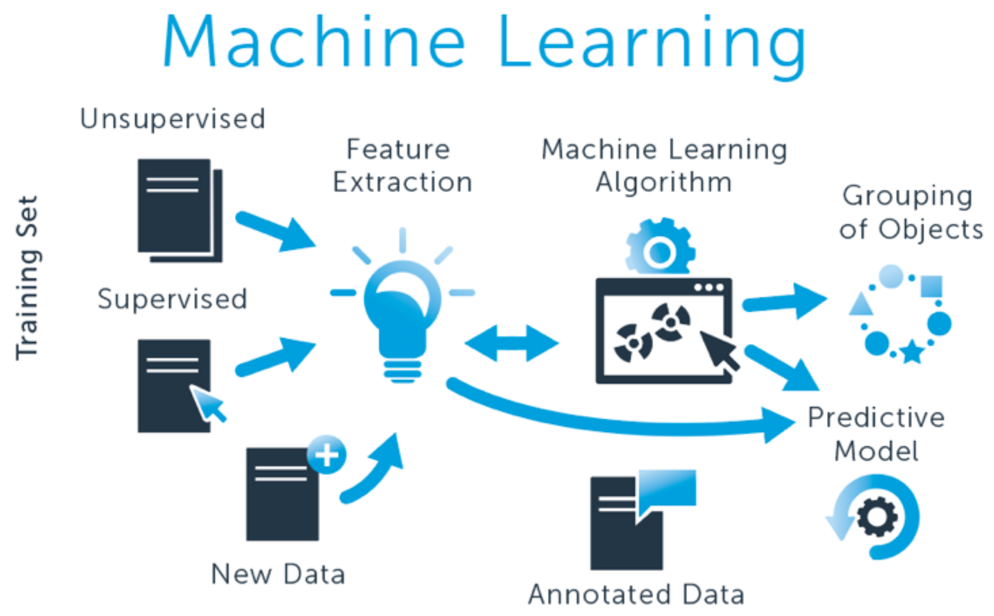
INTELLIGENCE IN NETWORK SECURITY

Intelligent Cybersecurity Methods and Architectures, Application of AI in IDS, SDN based Intelligent Network Security Solutions

INTELLIGENT SOFTWARE DEFINED SECURITY

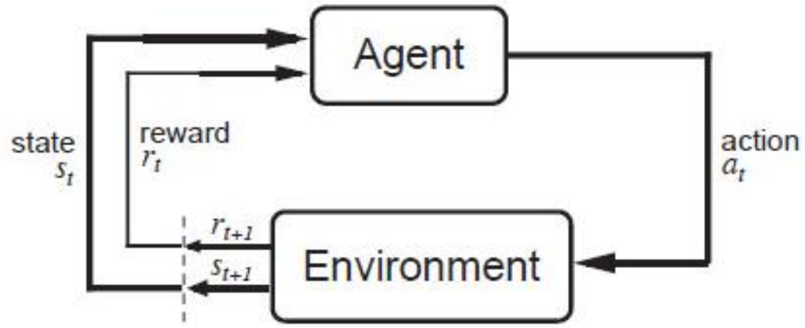
- Situation Awareness
- Self-Healing
- End-to-end Monitoring
- Network Analytic Capability
- Feedback mechanism to dynamically reconfigure the network

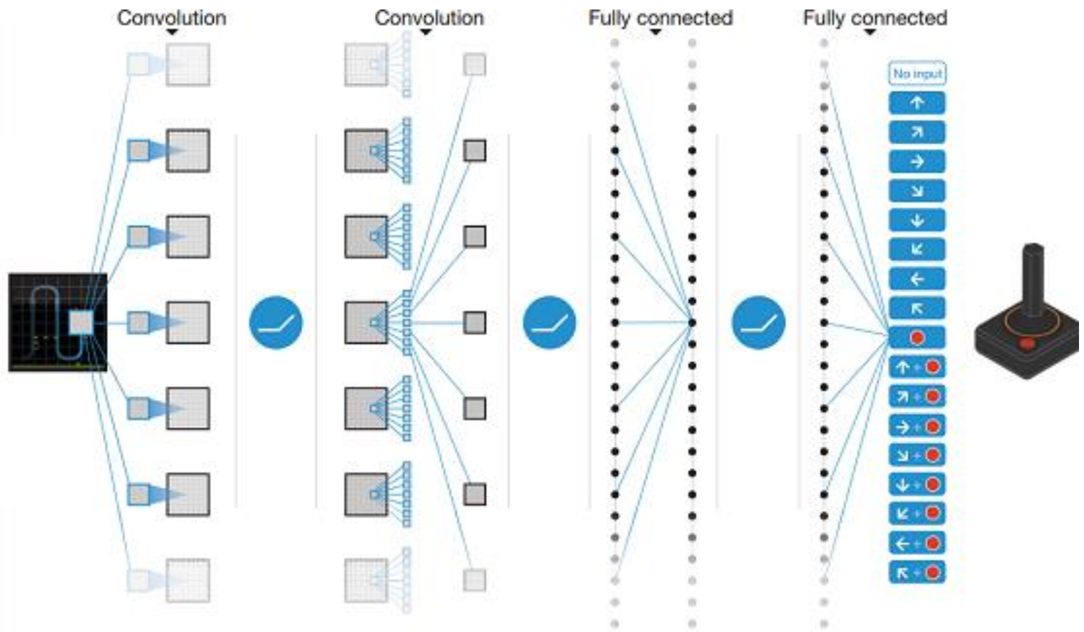
APPLICATION OF ML AND AI IN SECURITY



- **Machine Learning:** Statistical techniques to learn from available data without being programmed explicitly.

APPLICATION OF ML AND AI IN SECURITY





- Artificial Intelligence: Intelligent perception of the environment in order to take actions that maximize the chances of achieving the desired goal for the agent.

APPLICATION OF ML AND AI IN SECURITY

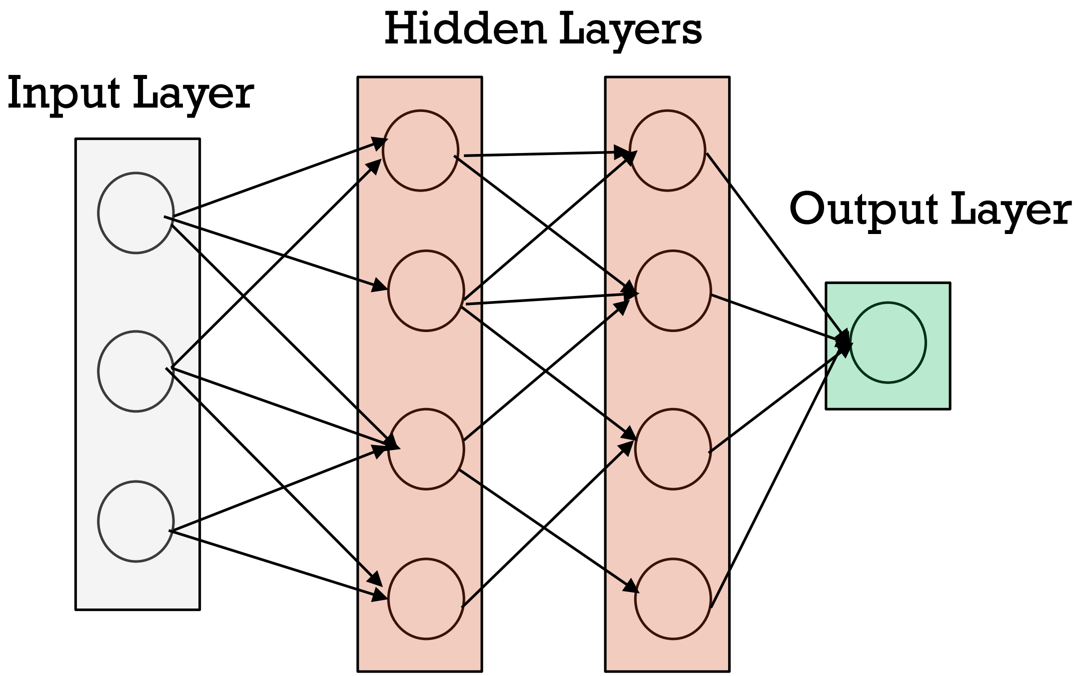
- AI mimics cognitive functions of human brain – Learning, Problem Solving.
- ML and AI algorithms working in tandem predict the usage patterns.
- Stealthy attacks can be detected, predicted and prevented using AI and ML based techniques.
- Proactive security based on AI can help in designing intelligent deception techniques – Honeypots.

INTELLIGENT CYBERSECURITY METHODS AND ARCHITECTURES

- Neural Networks
- Expert Systems
- Intelligent Agents
- Learning
- Search
- Constraint Solving

NEURAL NETWORKS

- Mimic the human cognition capabilities using a network of artificial neurons interacting with each other.
- Applications of NN include attack pattern recognition, intrusion detection, and prevention.



EXPERT SYSTEMS

- Modeling human reasoning with the aim of finding solutions to questions in application domains.
- Expert systems – (i) Knowledge Base (ii) Inference Engine.
- Knowledge Base stores expert knowledge.
- Inference Engine derives answers based on knowledge base.
- Security Planning, which involves selection of suitable security measures and optimal usage of limited security resources is an application area of expert systems in cybersecurity.

INTELLIGENT AGENTS

- Exhibit properties such as proactiveness, situation-awareness, communication with other intelligent agents.
- Cooperate and provide defense against problems such as distributed denial of service (DDoS).
- Multi-agent systems based hybrid and distributed Intrusion Detection Systems (IDS).

LEARNING

- Improving Intelligent systems by rearranging knowledge base and improving inference engine.
- Parameter Learning: Learning some parameters.
- Symbolic Learning: Grammar, concepts and user-behavior learning.
- Task classification: Supervised and Unsupervised Learning.

LEARNING

- Learning from large scale datasets – DDoS logs, user activity, system process data.
- Intrusion detection and threat analysis using Neural Networks and Self-Organized Maps (SOMs).

SEARCH

- Finding best solution from a list of candidate solutions.
- Utilization of additional knowledge to guide the search and improving the efficiency of the search.
- Stochastic Search, $\alpha\beta$-pruning can be utilized to solve security problems in an optimal fashion.
- Search algorithm can help the defender select a security configuration that guarantees maximum returns for the current security setting.

CONSTRAINT SOLVING

- Solving a set of constraints - equations, inequalities, logical statements for a problem.
- Planning problems in AI can be represented as Constraint Satisfiability Problems (CSP).
- Constraints restrict the search to a narrow dataset by taking into account information (security configuration) about a particular class of problem.

AI BASED INTRUSION DETECTION SYSTEM (IDS)

- AI-based expert systems can use training instances to acquire knowledge.
- Training Instances used in AI – (i) Rule-Based (ii) Classifier System.
- Rule-based Induction derives rules that are able to explain the training instances better than mathematical or statistical techniques.
- Classifier System utilize a set of training data in order to classify the future examples – Neural Network, Decision Tree.

AI BASED INTRUSION DETECTION SYSTEM (IDS)

- IDS should provide real-time analytic capability.
- Data reduction techniques used in AI data can optimize IDS performance.
- Real time attack prediction based on AI-based IDS.

IDS DATA REDUCTION

- User-activity will have some notable trends.

1. Filtering: AI-based input data-correlation can help in detection of usual activity and filtering unwanted data.
2. Feature Selection can help eliminate logs not having desired intrusion detection features.
3. Clustering can help in finding hidden patterns in data. Storing characteristics of the entire cluster.

IDS BEHAVIOR CLASSIFICATION

- IDS can identify only a certain fraction of intrusion events correctly.
- Normal users can often be flagged as malicious – False Positive and malicious users can pass undetected – False Negative.
- Statistical Anomaly Detection can help in improving the IDS classification performance.

IDS BEHAVIOR CLASSIFICATION

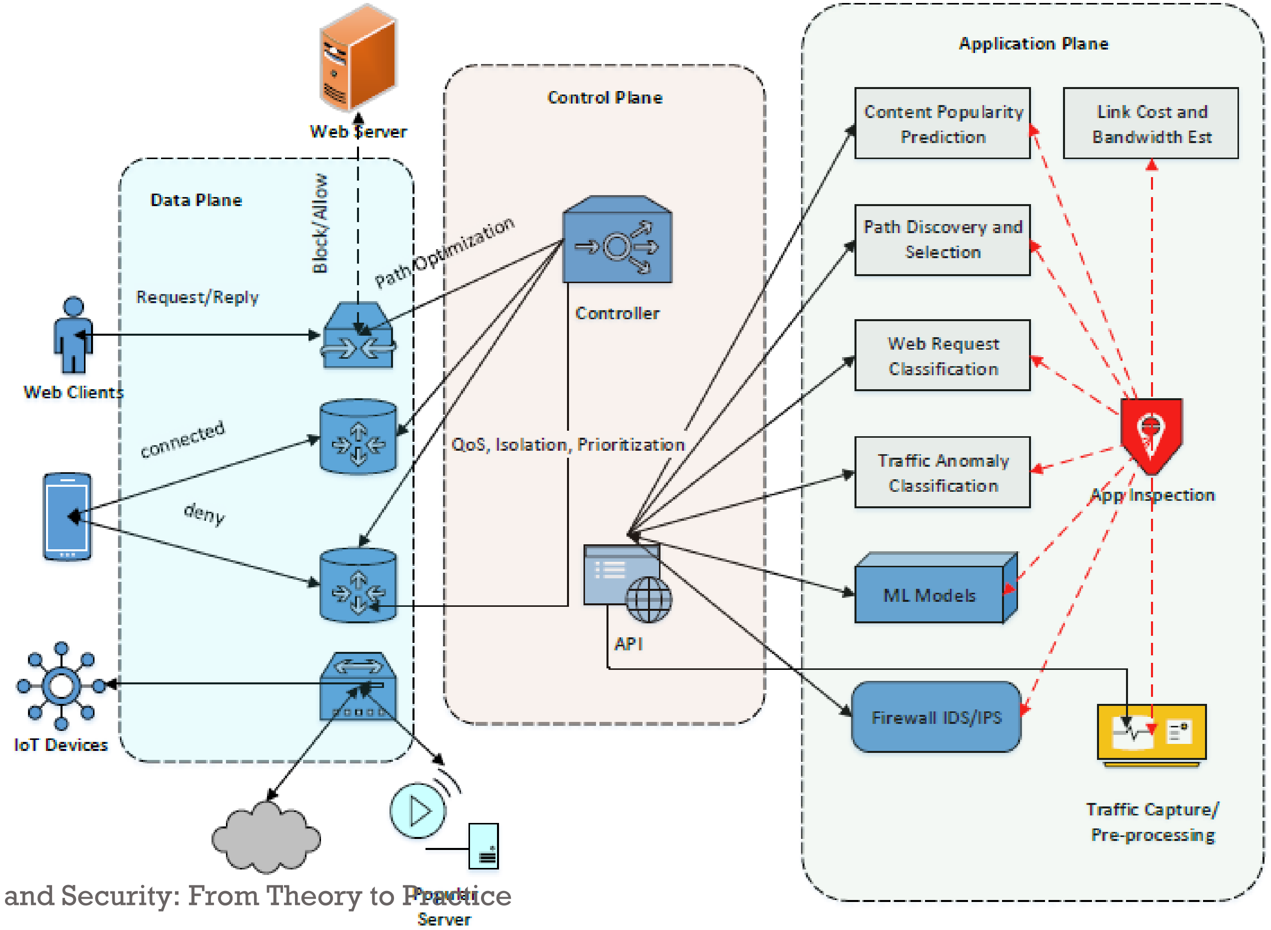
- Expert systems encode the known attacks and IDS policies as fixed set of rules.
- The user behavior is matched against the rules to determine the attacks.
- Rule encoding, which can be utilized to make conclusions regarding the information gathered by IDS.
- Domain expertise in expert systems provides optimal quality of rules.

IDS BEHAVIOR CLASSIFICATION

- Anomaly detection component compares the attacker's behavior against the normal expected user behavior.
- Phases of IDS:

1. Local information extraction.
2. Evolving background information from local abstraction.
3. Establishment of anomaly background boundaries.

SDN BASED INTELLIGENT NETWORK SECURITY



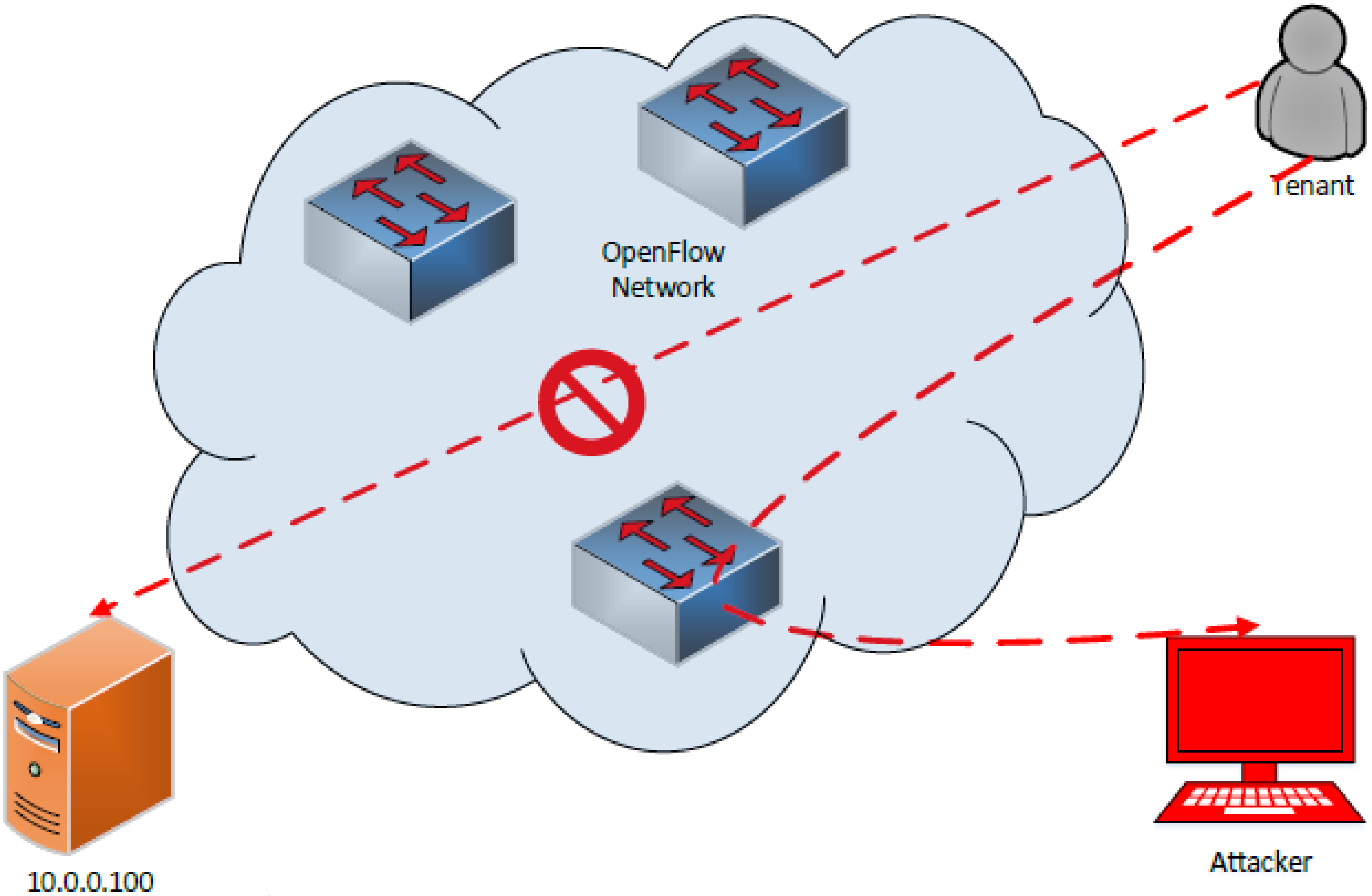
SDN BASED INTELLIGENT NETWORK SECURITY

- Centralized command and control.
- Flexibility, simplicity, and elasticity.
- Intelligent Application Plane – IDS/IPS, Traffic Anomaly Classification, Content Popularity prediction, Path Discovery.
- SDN controller acts as a middleware between intelligent application plane and data-plane.

SDN TOPOLOGY PROTECTION

- Attack Vector: Network Topology based attacks.
- With a poisoned topology, the visibility of upper layer services and apps may be misled by the attacker.
- E.g.- Man-in-the-middle (MiTM) attack, location hijacking, denial-of-service (DoS).
- Target: Link Discovery and Host tracking service APIs of SDN controllers – NOX, POX, ODL.

HOST LOCATION HIJACKING



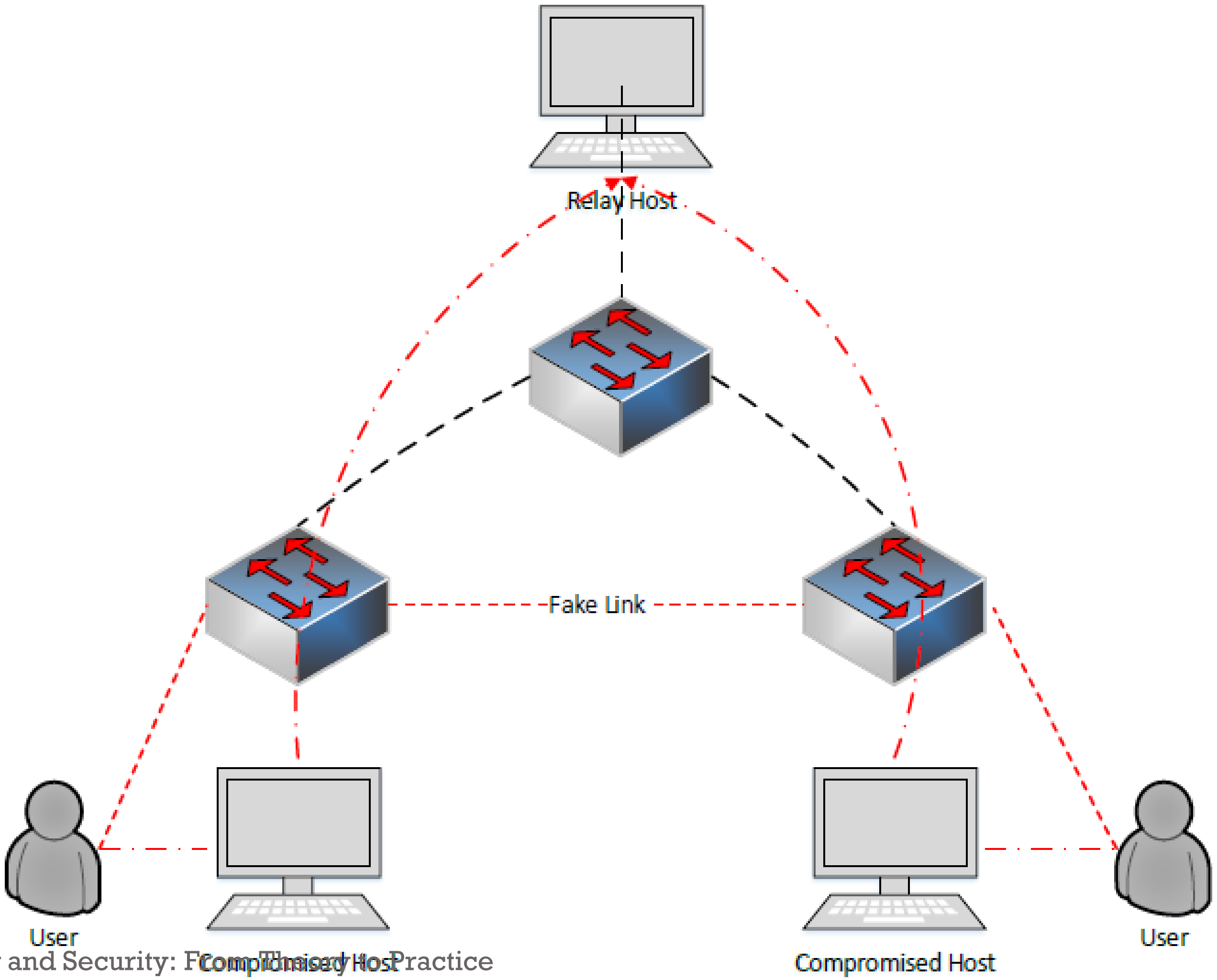
HOST LOCATION HIJACKING

- Host Tracking System (HTS) can identify events such as host location migration.
- Existing SDN controllers such as OpenDaylight (ODL) have weak security for host location update service.
- ODL has API *isEntityAllowed* which accepts any host location update.

HOST LOCATION HIJACKING

- The packet forwarding and routing decisions are made by SDN controller using host location information.
- An attacker can tamper with host location information impersonating the target host.
- Attacker can hijack the traffic directed towards the legitimate host.

LINK FABRICATION ATTACK



LINK FABRICATION ATTACK

- Links between various switches are discovered using Link Layer Discovery Protocol (LLDP).
- Open Flow Discovery Protocol (OFDP) and Link Discovery Service (LDS) in addition to LLDP are used by OpenFlow controller to construct network topology.
- Security Flaw in link discovery can be exploited by the malicious attacker.

LINK FABRICATION ATTACK

- LDS specification security constraints:

1. Integrity/origin of LLDP packets must be ensured in link discovery procedure.
2. Propagation path of LLDP packets must only contain OpenFlow-enabled switches.

- Incorrect enforcement of constraints opens up a window of opportunity for the attacker.

LINK FABRICATION ATTACK

- Adversary can craft falsified LLDP packets.
- Adversary can relay LLDP packets between switches in order to fabricate a fake internal link.
- Adversary can receive LLDP packets from one target switch and repeat it to another target switch without modification.
- This attack can serve as a basis of DoS or MITM attack.

STATIC DEFENSE AGAINST TOPOLOGY POISONING ATTACKS

- Configuring host link and location information beforehand.
- Manually verifying/updating the information when required.
- Error-prone and difficult to scale on a large network.

DYNAMIC DEFENSE AGAINST HOST LOCATION HIJACKING

- Authentication of host information using public-key infrastructure (PKI).
- The location information update can be embedded in unused packet field (VLAN or ToS).
- Checking pre-condition of host migration *Port_Down* and post-condition migrated host-entity is unreachable in the previous location.

DYNAMIC DEFENSE AGAINST LINK FABRICATION

- Adding additional authentication in LLDP packet. The digital signature can be calculated over the semantics of LLDP packet (DPID and Port number).
- Switch property verification to check if host resides inside LLDP propagation, e.g., traffic coming from switch port can be inspected to check connected devices.
- Replay Attack Protection: LLDP packets can only transmit only on switch internal link ports and ports connected to SDN controller.

SDN-ML BASED DOS PROTECTION

- Traffic logs can be processed to identify statistics utilized by ML models.
- Control plane can query traffic statistics related to forwarded traffic.
- Malicious attack pattern can be identified by ML algorithm.
- Bad traffic can either be dropped or forwarded to Remote Triggered Black Hole (RTBH) routing component.

ADVANCED PERSISTENT THREATS (APT)

Traditional Attacks vs APT, APT Attack Model, APT Case Studies, APT Detection/Mitigation, Orchestrating SDN to disrupt APT

ADVANCED

- The APT attacks are well funded and use advanced mode of operations, sophisticated tools.
- The advanced tools employ multiple attack vectors.
- Target organization often carries a high value.

PERSISTENT

- Highly motivated and persistent attackers.
- Once the attackers gain access into the system, they try to gain access to connected systems.
- Slow and low approach.
- The attacker employ several evasive techniques to prevent triggering of security alarms.

THREAT

- The threat in case of APT attack is a loss of data or critical information.
- Disruption in the normal operations of an organization.
- Loss of reputation and mission-critical information.
- Threats are difficult to detect, end requires sophisticated defense mechanisms to detect and prevent.

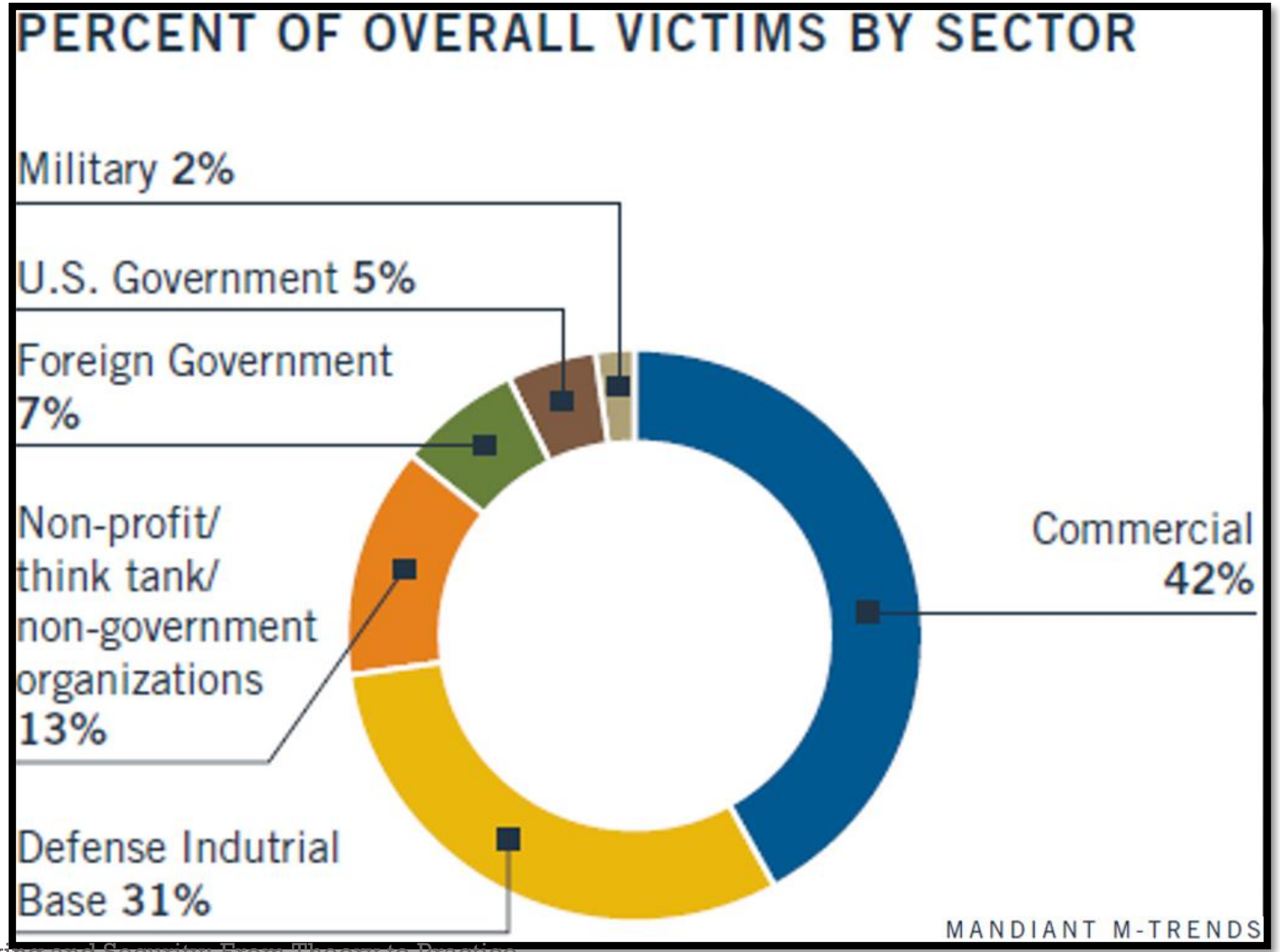
NIST APT ATTACKER DEFINITION

- Pursues its objectives repeatedly over an extended period.
- Adapts to defenders' efforts to resist it.
- Is determined to maintain the level of interaction needed to execute its objective.

APT KEY CONTRIBUTORS

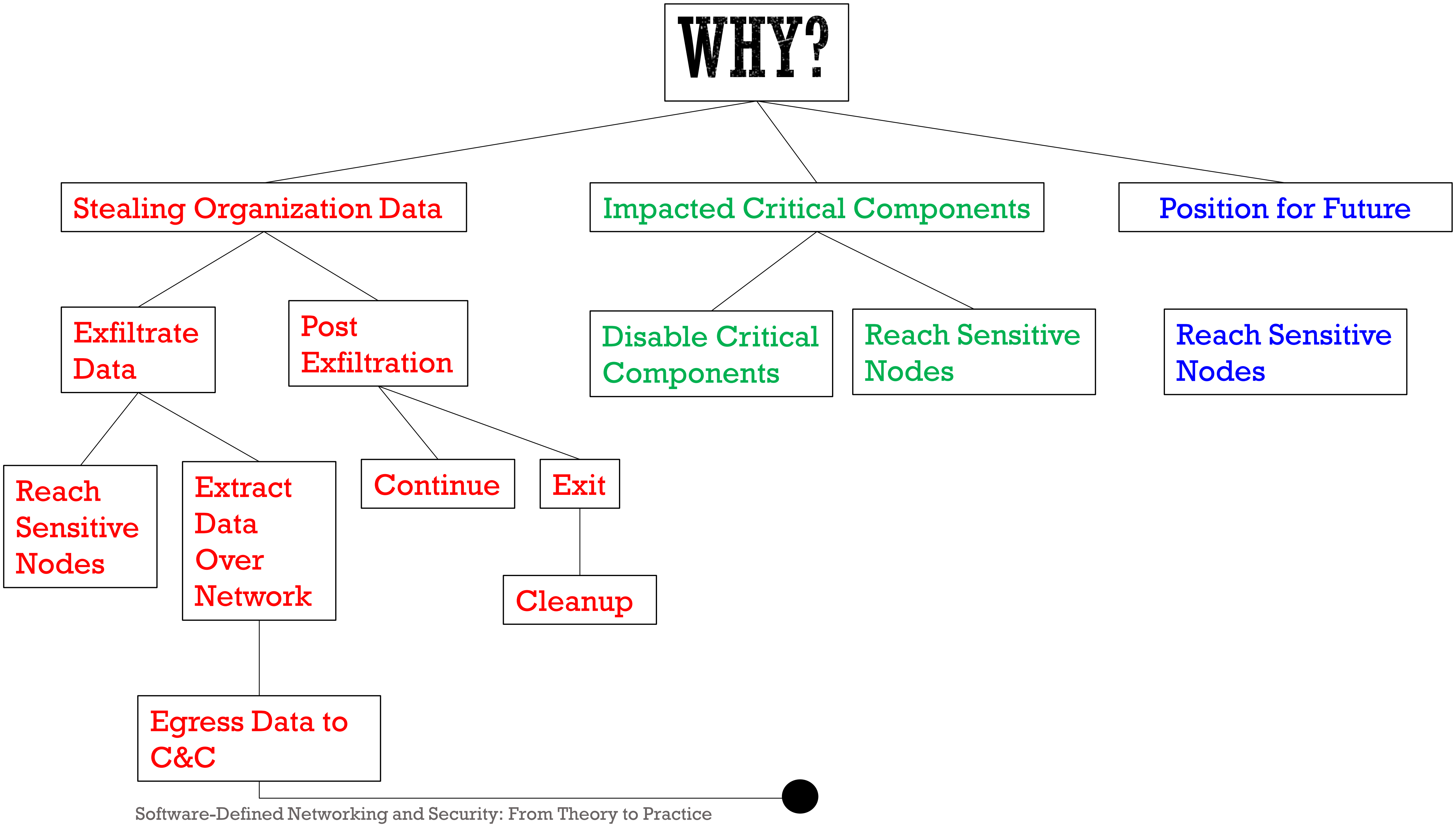
- Nation States
- Organized crime groups
- Hacktivist Groups

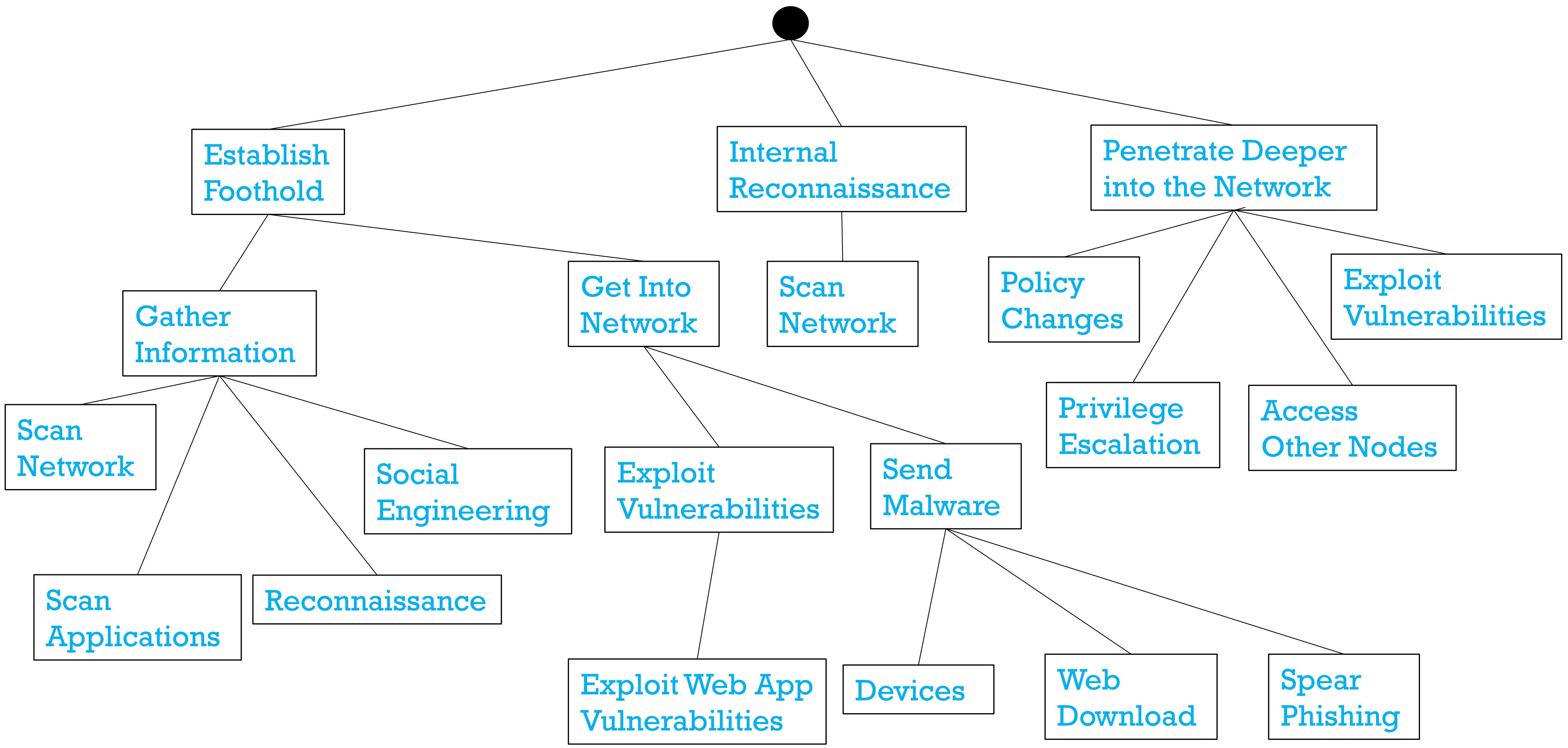
APT IMPACTED SECTORS



APT IMPACTED SECTORS

Commercial Sector Breakdown	%
Automotive	2
Space Satellite and Imagery	19
Cryptography & Communications	20
Mining	2
Energy	18
Legal	9
Investment Banking	3
Media/PR	10
Hospital	2
Chemical	5
Technology	10


WHY?
Stealing Organization Data
Impacted Critical Components
Position for Future
Exfiltrate Data
Post Exfiltration
Disable Critical Components
Reach Sensitive Nodes
Reach Sensitive Nodes
Reach Sensitive Nodes
Extract Data Over Network
Continue
Exit
Cleanup
Egress Data to C&C



Establish Foothold
Internal Reconnaissance
Penetrate Deeper into the Network
Gather Information
Get Into Network
Scan Network
Policy Changes
Exploit Vulnerabilities
Privilege Escalation
Access Other Nodes
Scan Network
Social Engineering
Exploit Vulnerabilities
Send Malware
Scan Applications
Reconnaissance
Exploit Web App Vulnerabilities
Devices
Web Download
Spear Phishing

CASE STUDY: EQUIFAX

- One of the major credit bureaus became a victim to what they claimed as APT attack in 2017.
- One of the largest data breaches in history where the data of 143 million people were exposed for more than three months.
- Attackers exploited an unpatched vulnerability in Apache Struts Code.
- NIST published this vulnerability with a score of 10.0, the highest score a vulnerability can be assigned.
- Is this an APT attack ?

WAS EQUIFAX HACK AN APT?

- NO. The attack was NOT an APT attack, it was a targeted data breach attack.
- One of the systems in Equifax wasn't patched on this vulnerability.
- Attackers took control of the portal website that uses this Apache Struts software.
- From that web server, they went onto database server, and exfiltrated the data.

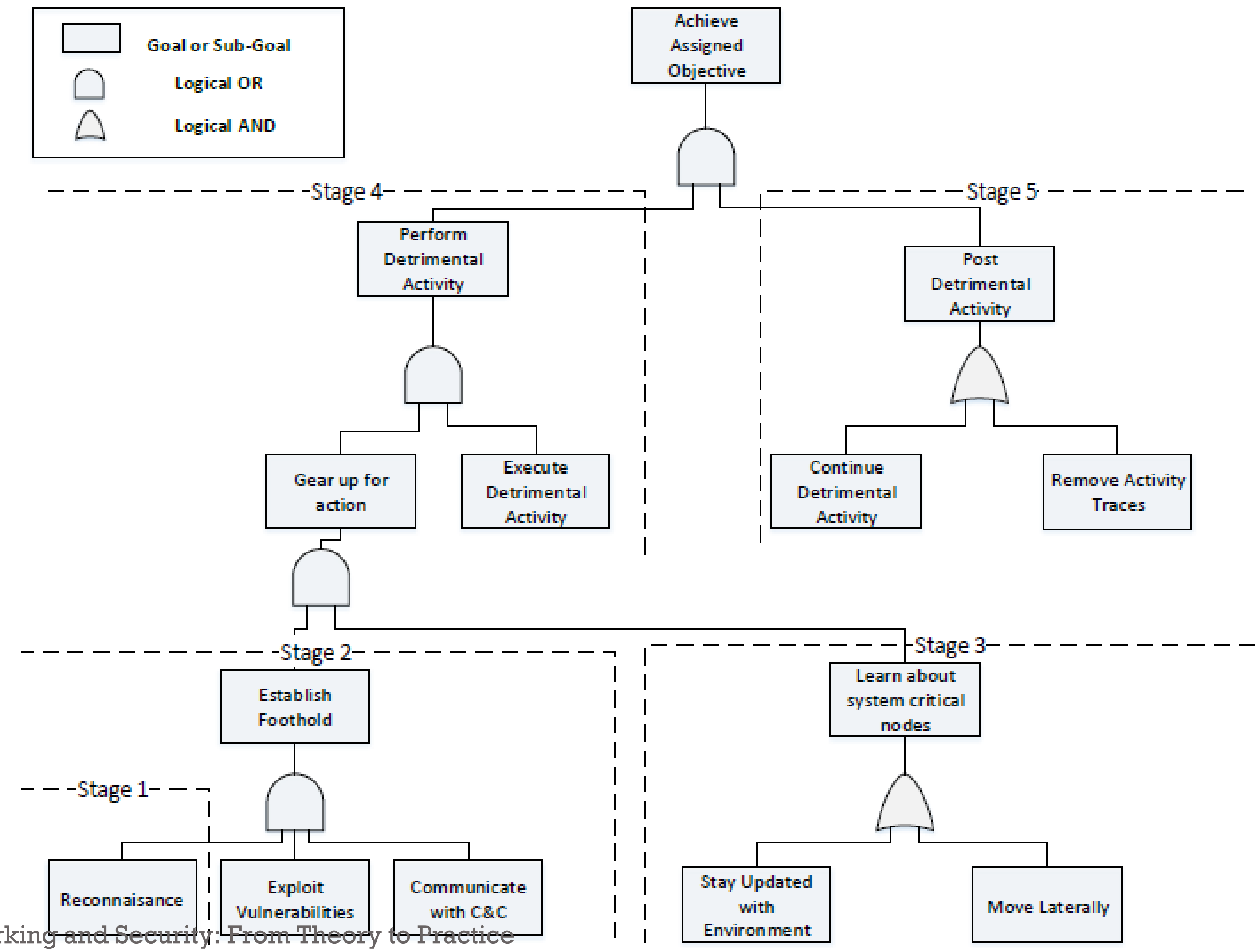
WAS EQUIFAX HACK AN APT?

- Neither the level of sophistication not the attackers' attempt to stay undetected was part of the plan.
- It was merely a grab and go attack.
- Equifax failed to detect the unpatched vulnerability, failed to patch the vulnerability, failed to detect the compromise of their web server and failed to detect huge volumes of data going out of their network.

TRADITIONAL ATTACKS VS APT

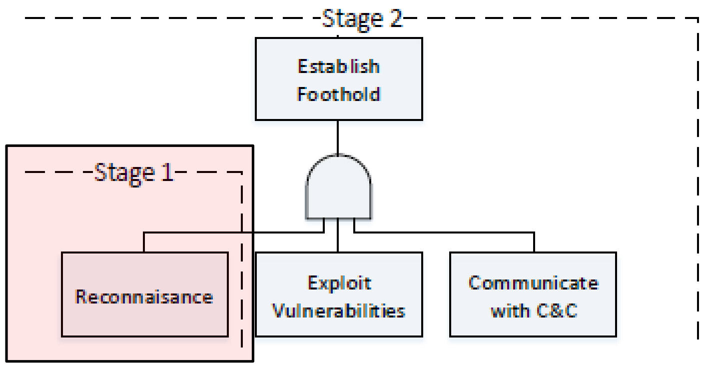
	Traditional Attacks	APT Attacks
Attacker	Mostly single person	Highly organized, sophisticated, determined, and well-resourced group
Target	Unspecified, mostly individual Systems	Specific organizations, governmental institutions, commercial enterprises
Purpose	Financial benefits, demonstrating abilities	Competitive advantages, strategic benefits
Approach	Single-run,“ smash and grab", short Period	Repeated attempts, stays low and slow, adapts to resist defenses, long term

STAGES OF APT



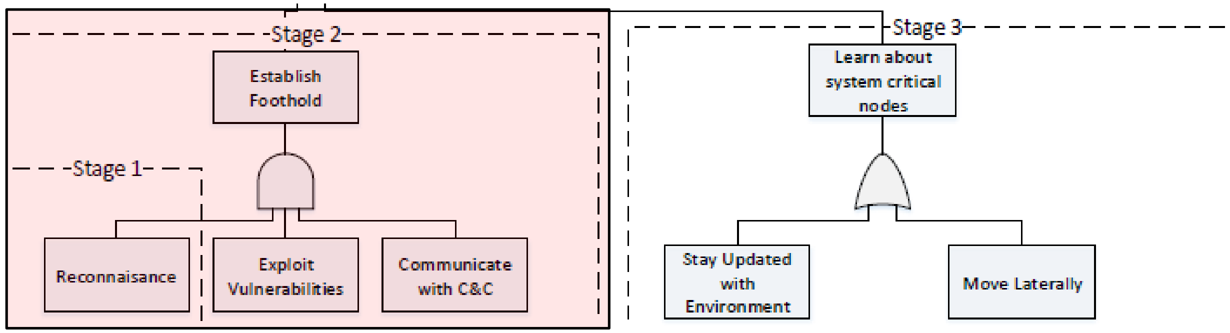
RECONNAISSANCE

- Attacker tries to gather a lot of information about the target.
- E.g., - details of employees of the target organization such as social life, websites visited, habits of the employee.
- The information can help attackers to easily establish the foothold into the target network.



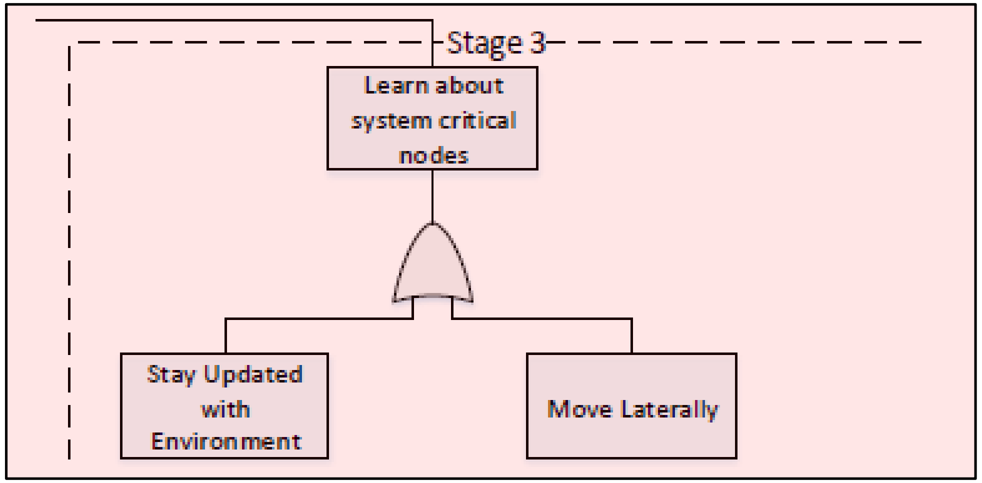
FOOTHOLD ESTABLISHMENT

- Exploit the vulnerabilities found in the target organization's web application, databases, and other software.
- Vulnerabilities from known sources NVD database, dark-web and deep-web forums.
- Social engineering, Business Email Compromise scams, phishing emails.
- Techniques as help attacker establish a foothold in the network.



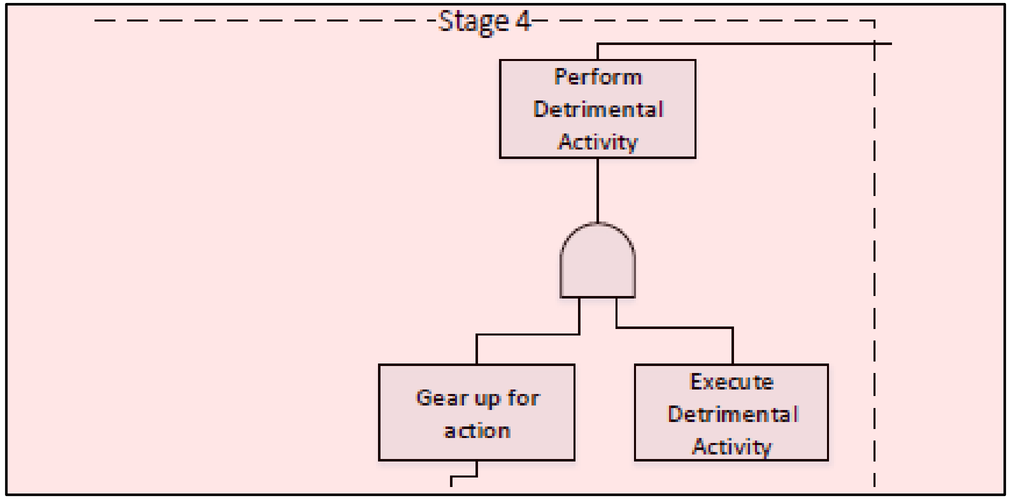
LATERAL MOVEMENT (SLOW AND LOW)

- Lateral movement, access to other sensitive hosts.
- E.g. - Malware can spread to the neighboring machines in the target environment.
- Goal: Expand the foothold to other systems in search of the data they want to exfiltrate.
- Methods Used: user account Password Dumping, Hash Dumping
- Tools Used: WCE, Mimikatz, Windows LSA.



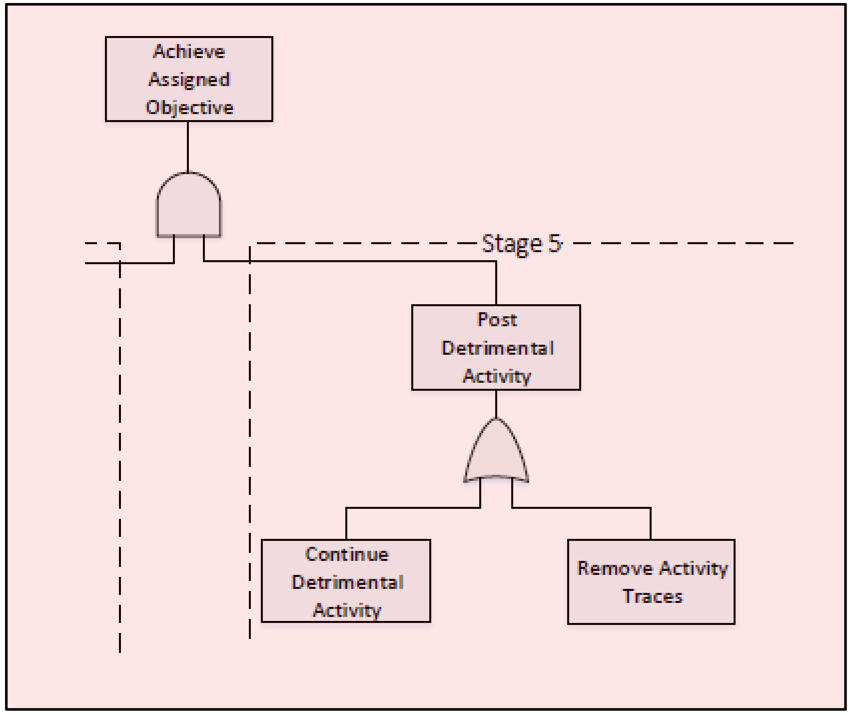
EXFILTRATION/IMPEDIMENT

- Exfiltrate the data collected to their command and control center.
- The IDPS do ingress filtering and not egress filtering, data-exfiltration often goes undetected.
- The attacker may split the exfiltrated data into batches and distribute exfiltration over a long period of time.



POST-EXFILTRATION/POST-IMPEDIMENT

- Maintain the persistence until the attack has been lifted by the attack sponsor.
- Cover tracks to prevent forensic analysis.
- Delete service and system activity logs.



APT ATTACKS

- **Hydraq** - One of the first APT attacks on commercial companies that has drawn great attention.
- **Stuxnet** - A sophisticated worm that spread itself to other components in the entity with a goal to impede Iran's uranium nuclear project.
- **RSA Secure ID Attack** - Another attack that infiltrated an organization's network through phishing emails sent to the organization's employers.

HYDRAQ

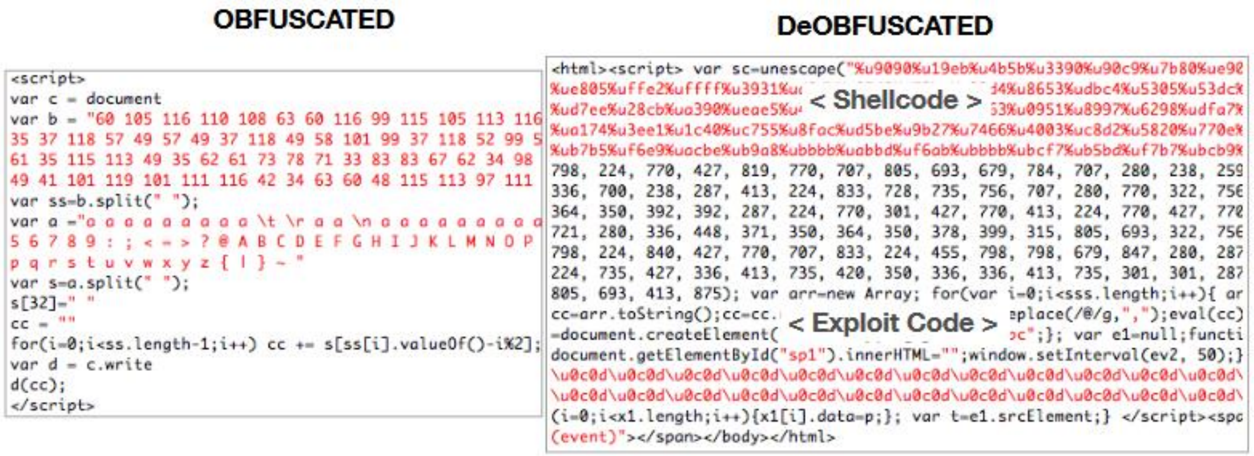
- Well known under the original name **Operation Aurora.**
- Several versions were identified, common in all those is the Trojan called as Hydraq that establishes a backdoor on the victim's system
- Earlier versions exploited zero-day vulnerability in Adobe reader and acrobat products.

HYDRAQ

- Attack targeted at Google involved exploitation of a zero-day vulnerability in Internet Explorer.
- Later versions were found to no longer use zero-day vulnerabilities.
- Successful in establishing foothold in networks of several organizations.

HYDRAQ ANALYSIS

- Social engineering tricks can then be deployed to entice target users.
- Exploits 0-Day vulnerabilities CVE-2010-0249 and MS10-002 in IE.
- JavaScript to conceal the code's real intentions.



HYDRAQ IE EXPLOIT ROUTINE

- IE HTML object handling flaw.
- IE tries to access deleted or incorrectly initialized HTML object.
- Hydraq binary shellcode is executed on the target system.

```
var e1=null;
function ev1(evt)
{
 e1=document.createEventObject(evt);
 document.getElementById("sp1").innerHTML="";
 window.setInterval(ev2, 50);
}
function ev2()
{
p="\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\
u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0
d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0
c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d"
;
for(i=0;i<x1.length;i++){x1[i].data=p;};
var t=e1.srcElement;
}
```

HYDRAQ BINARY SHELLCODE

- Hydraq shell code is u% encoded.
- Bitwise XOR with the key 0xD8 reveals the hidden instruction.
- Inspection of the decoded shellcode shows the location where Hydraq installer is stored, .e.g- C:\Documents and Settings\<user>\Application Data\installer.exe

```
<html><script> var
sc=unescape("%u9090%u19eb%u4b5b%u3
390%u90c9%u7b80%ue901%u0175%u66c3%
```

```
01012475 > $ 90            NOP
01012476   . 90            NOP
01012477   . EB 19         JMP SHORT calc.01012492
01012479   $ 5B            POP EBX
0101247A   . 4B            DEC EBX
0101247B   . 90            NOP
0101247C   . 33C9          XOR ECX,ECX
0101247E   . 90            NOP
0101247F   . 807B 01 E9    CMP BYTE PTR DS:[EBX+1],0E9
01012483   . 75 01         JNZ SHORT calc.01012486
01012485   . C3            RETN
01012486   > 66:B9 7B04    MOV CX,47B
0101248A   > 80340B D8     XOR BYTE PTR DS:[EBX+ECX],0D8
0101248E   .^E2 FA         LOOPD SHORT calc.0101248A
01012490   . EB 05         JMP SHORT calc.01012497
01012492   > E8 E2FFFFFF   CALL calc.01012479
```

HYDRAQ MAINTAINING ACCESS

- Win32/Hydraq dropper generates a random service name.

Ups<3 random characters>

- Drops the DLL component from its resource to %System%\Rasmon.dll.
- Adds generated service name to the registry entry

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SvcHost\SysIns

HYDRAQ MAINTAINING ACCESS

- Create and enable service with characteristics below:

```
ServiceName = "Ups<3 random characters>"
DesiredAccess = SERVICE_ALL_ACCESS
ServiceType = SERVICE_WIN32_SHARE_PROCESS
StartType = SERVICE_AUTO_START
ErrorControl = SERVICE_ERROR_NORMAL
BinaryPathName = "%SystemRoot%\System32\svchost.exe -k SysIns"
```

- Using this service the DLL component will be executed under context of generic host process svchost.exe.

HYDRAQ DELETING INSTALLATION TRACES

- The installation traces in registry are deleted by Hydraq dropper.
- Data below is deleted from the registry.
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SvcHost\SysIns.
- The dropper component creates and executes a batch file in %Windows%\DFS.bat.
- This batch file deletes the Hydraq dropper file.

STUXNET

- A sophisticated malware.
- 4 zero-day vulnerabilities
- 2 stolen certificates.
- 2 command and control centers.

STUXNET

- Cleverly crafted, layered malware.
- Tweaked by attackers from their command and control centers using over 400 items in the malware configuration file.
- It was found to end 3 years after it was unleashed.
- The worm infected 200,000 computers in the nuclear plant, causing 1000 machines to physically degrade.

STUXNET

- Stuxnet consists of three modules;

1. Worm that executed the routines related to the main attack payload.
2. Link file that auto-executes the propagated copies of the worm.
3. Rootkit component that is responsible for hiding the activities of malicious processes and les, thus preventing the discovery of the worm.

STUXNET INJECTION TECHNIQUE

- Enumerate currently running processes to identify the following:

1. Kaspersky (avp.exe)
2. McAfee (avguard.exe)
3. AntiVir (avguard.exe)

- Search Registry files for Antivirus programs:

1. KAV v6-9
2. McAfee

STUXNET INJECTION TECHNIQUE

- Based on the version number of security product, injection process is identified. If security product is non-bypassable, injection process fails.
- Target processes for injection:

1. sass.exe
2. Winlogon.exe
3. Svchost.exe
4. The installed security product process

CONFIGURATION DATA BLOCK

- Contains all the values used to control how Stuxnet will act on a compromised computer.
- When a new version is created, configuration data block is updated and computer description block is appended to data block.
- Computer Description Block

5.1 - 1/1/0 - 2 - 2010/09/22-15:15:47 127.0.0.1, [COMPUTER NAME] [DOMAIN NAME] [c:\a\1.zip:\proj.s7p]

STUXNET INSTALLATION

- Export 15 is the first export called when the .dll file is loaded for the first time.
- Responsible for checking that the threat is running on a compatible version of Windows, checking whether the computer is already infected or not, elevating the privilege of the current process to system.
- It then injects the .dll file into the chosen process using a unique injection technique described in the Injection Technique section and calls export 16.

STUXNET INSTALLATION

- Export 16 is the main installer for Stuxnet.
- It checks the date and the version number of the compromised computer; decrypts, creates and installs the rootkit files and registry keys.
- Injects itself into the services.exe process to infect removable drives.
- Injects itself into the Step7 process to infect all Step 7 project
- Establishes communication between different modules using global mutex, and connects to RPC server.

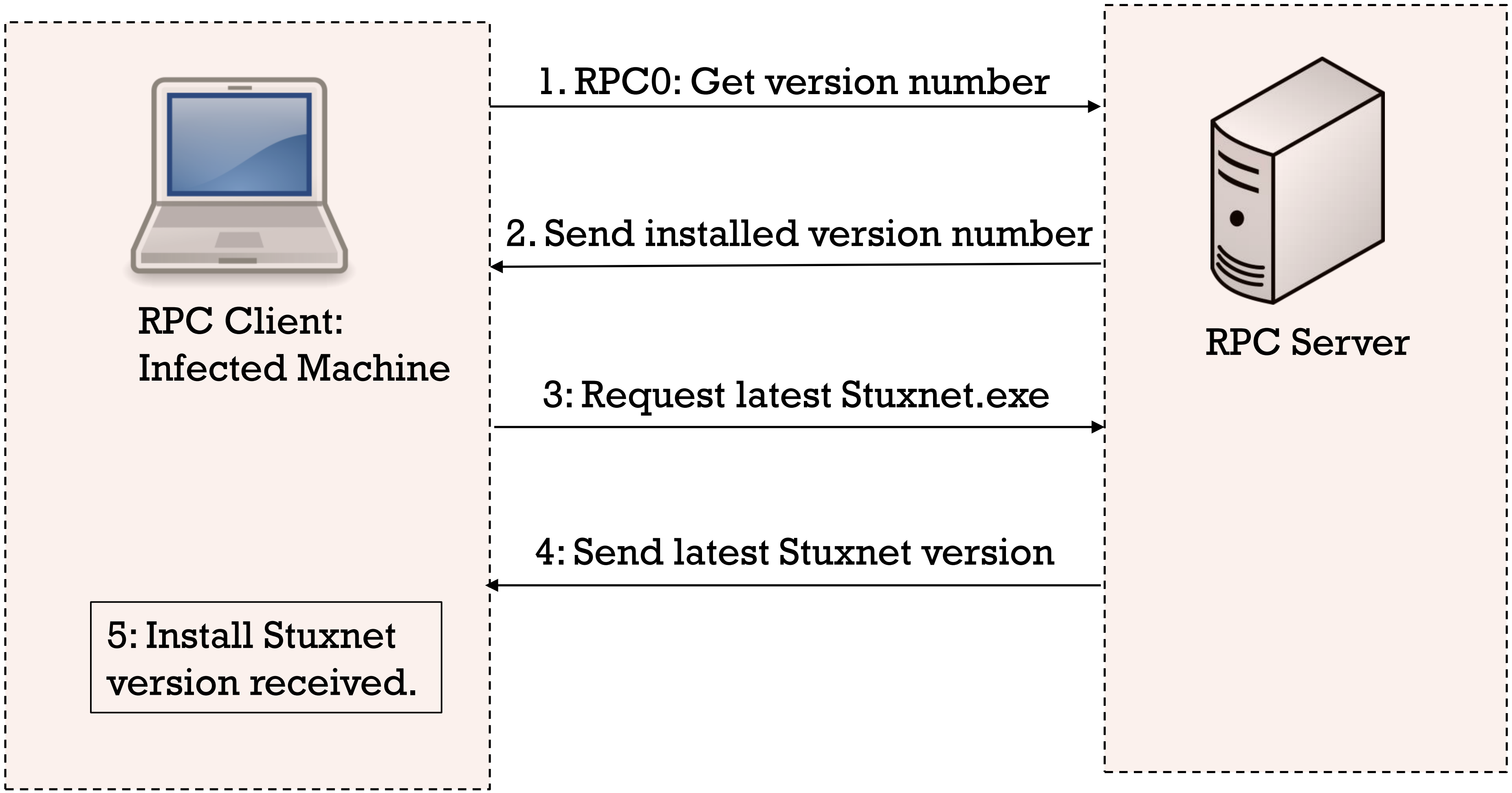
STUXNET C&C

- Stuxnet connects to command and control server on port 80 and sends some basic information about the compromised computer to the attacker via HTTP.

1. www[.]mypremierfutbol[.]com – Denmark Server
2. www[.]todaysfutbol[.]com – Malaysia Server

- The threat has the capability to update itself with new command and control domains.
- Send the payload to a target server. Target 0-Day vulnerability (MS10-073) on IE process to achieve local privilege escalation.

STUXNET COMMUNICATION EXAMPLE



STUXNET – PUTTING IT ALL TOGETHER

0: Returns the version number of Stuxnet installed

1: Receive an .exe file and execute it (through injection)

2: Load module and executed export

3: Inject code into lsass.exe and run it

4: Builds the latest version of Stuxnet and sends to compromised computer

5: Create process

6: Read file

7: Drop file

8: Delete file

9: Write data records

RSA SECURE ID ATTACK

- Compromise of information associated with RSA's SecureID product, a 2-factor token authentication system.
- 2 different, well-crafted phishing emails.
- Email sent to 2 different groups of employees with an excel sheet.
- Backdoor that gives remote access to the attackers.

RSA SECURE ID ATTACK

- Harvested credentials.
- Performed privilege escalations.
- Stole the data and files.
- Compressed and encrypted the data before sending it over ftp to their command and control center.

APT DETECTION/MITIGATION

- No single IDS will suffice to protect against APT attacks.
- A framework compromising of at the least Signature Based and Anomaly Based Detection systems should be used.
- Signature Based Solutions will detect known vulnerabilities.
- Anomaly based detectors can detect zero-day vulnerabilities.

APT DETECTION/ MITIGATION

- Monitoring for different user activities and how the data moves within and outside of the network.
- Correlation of different activities reported by different agents across the network.
- Employing machine learning methodologies such as supervised, unsupervised and semi-supervised as necessary during the data collection and correlation.

APT DETECTION/MITIGATION

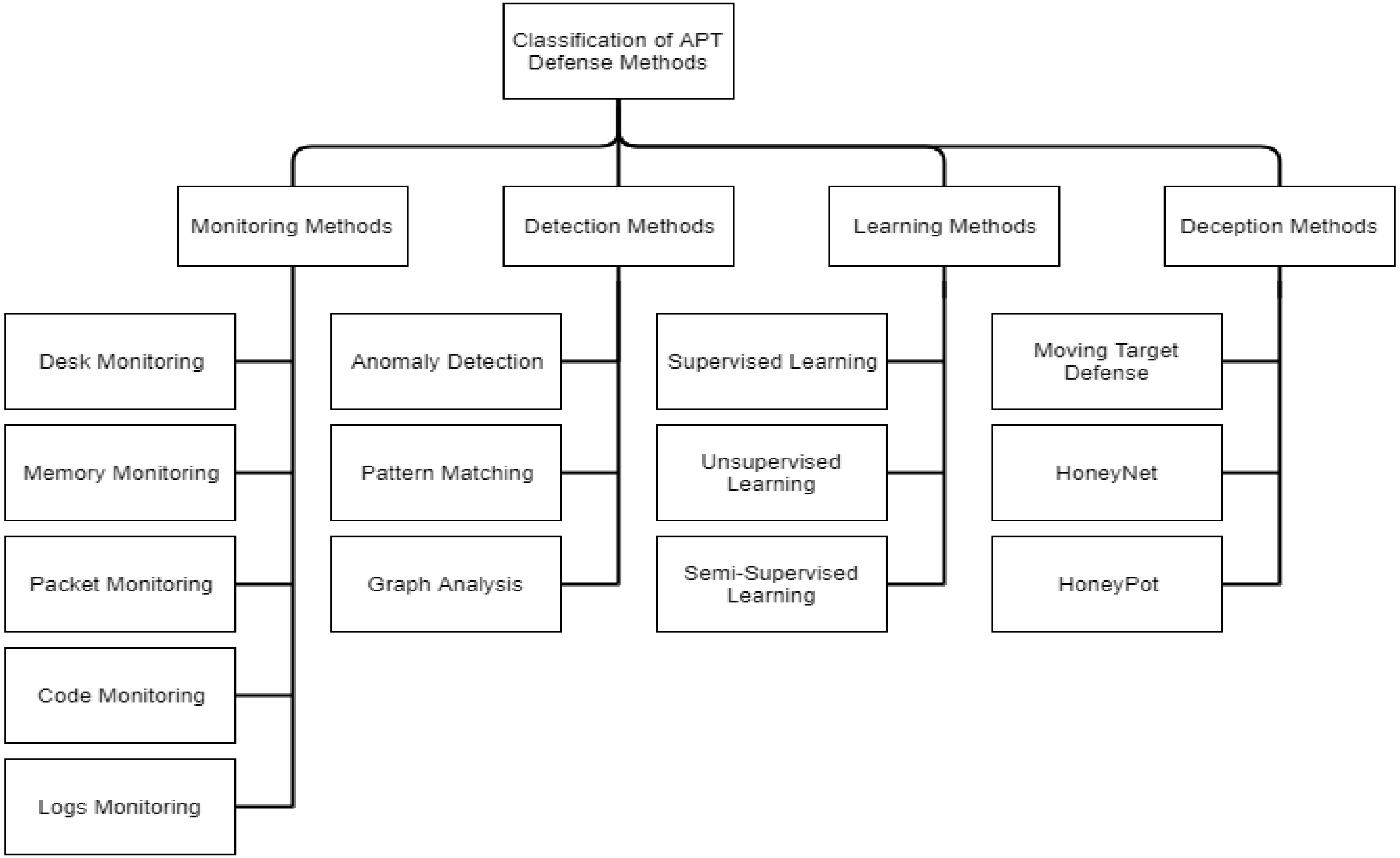
- Symantec's Advanced Threat Protection (ATP) that contains network, endpoint, email and roaming security methods.
- Forcepoint utilizes Data Loss Protection (DLP), malware protection, insider threat detection and next-generation firewall (NGFW) based security enforcement.
- Other techniques includes application whitelisting, patching vulnerabilities, restricting admin access to OS and applications.

APT DETECTION/MITIGATION

- Monitoring Methods
- Detection Methods
- Mitigation Methods

1. Learning Methods
2. Deception Methods

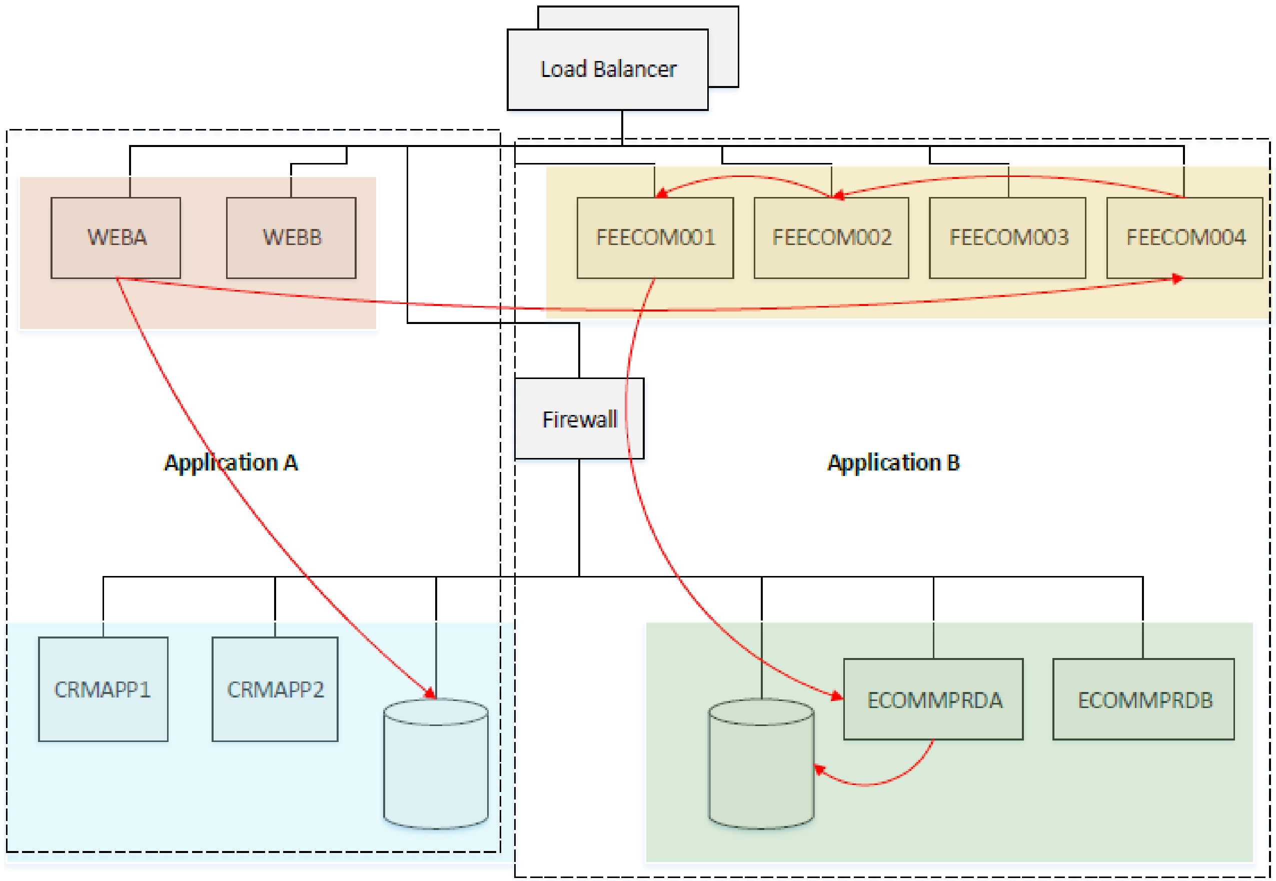
APT DEFENSE METHODS



SDN BASED APT PROTECTION

- Centralized command and control, network-wide visibility helps in taking preventive actions.
- Micro-segmentation.
- Service Function Chaining.
- Granular attack analysis, breaking lateral movement of the attacker.

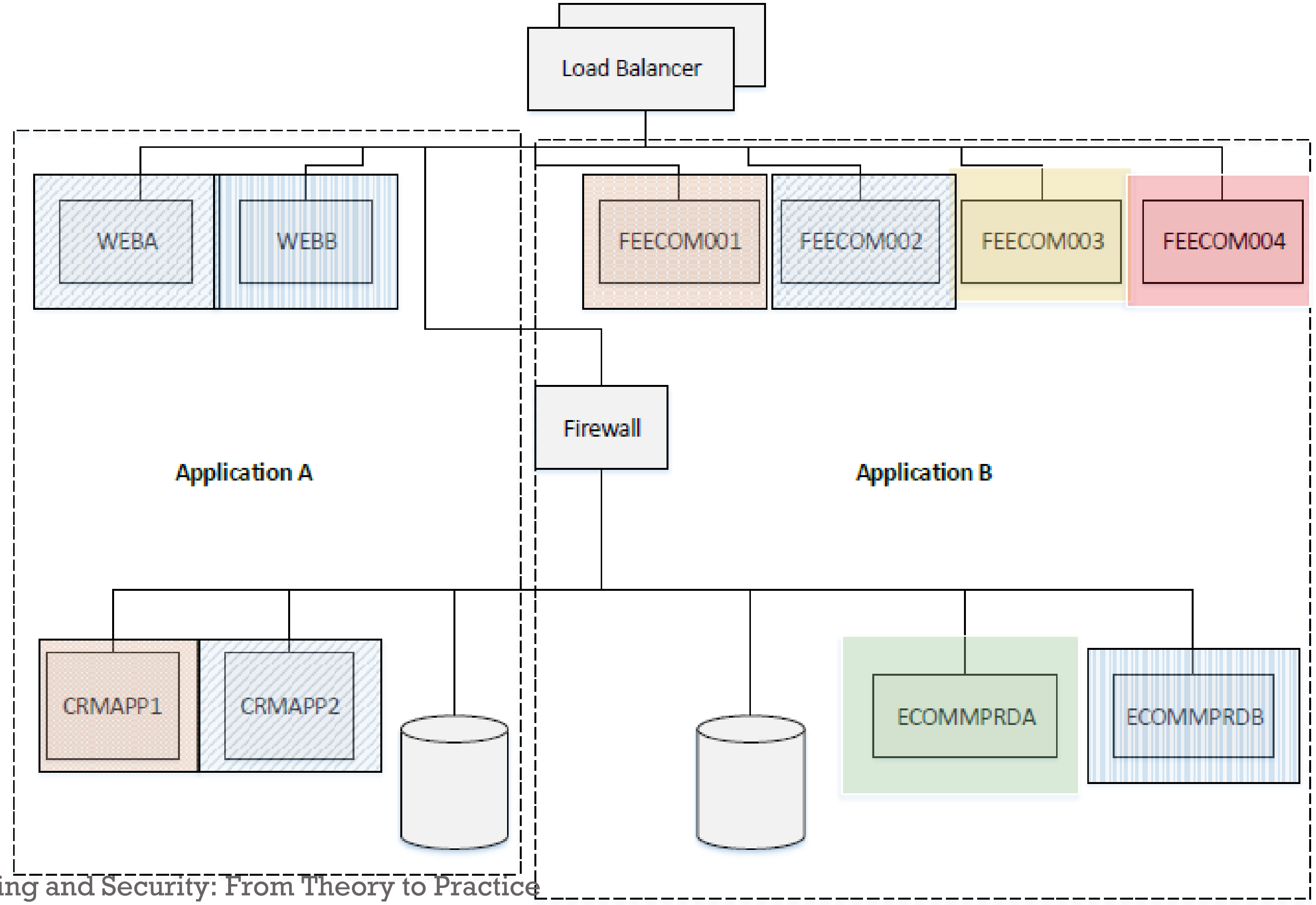
APT LATERAL MOVEMENT EXAMPLE



APT LATERAL MOVEMENT EXAMPLE

- Attacker can exploit the Web Server.
- Application Server A and uses the elevated privileges to exploit the communication server present on the application Server B.
- Applications present on the adjacent networks can be targeted by the attacker in a multi-stage attack

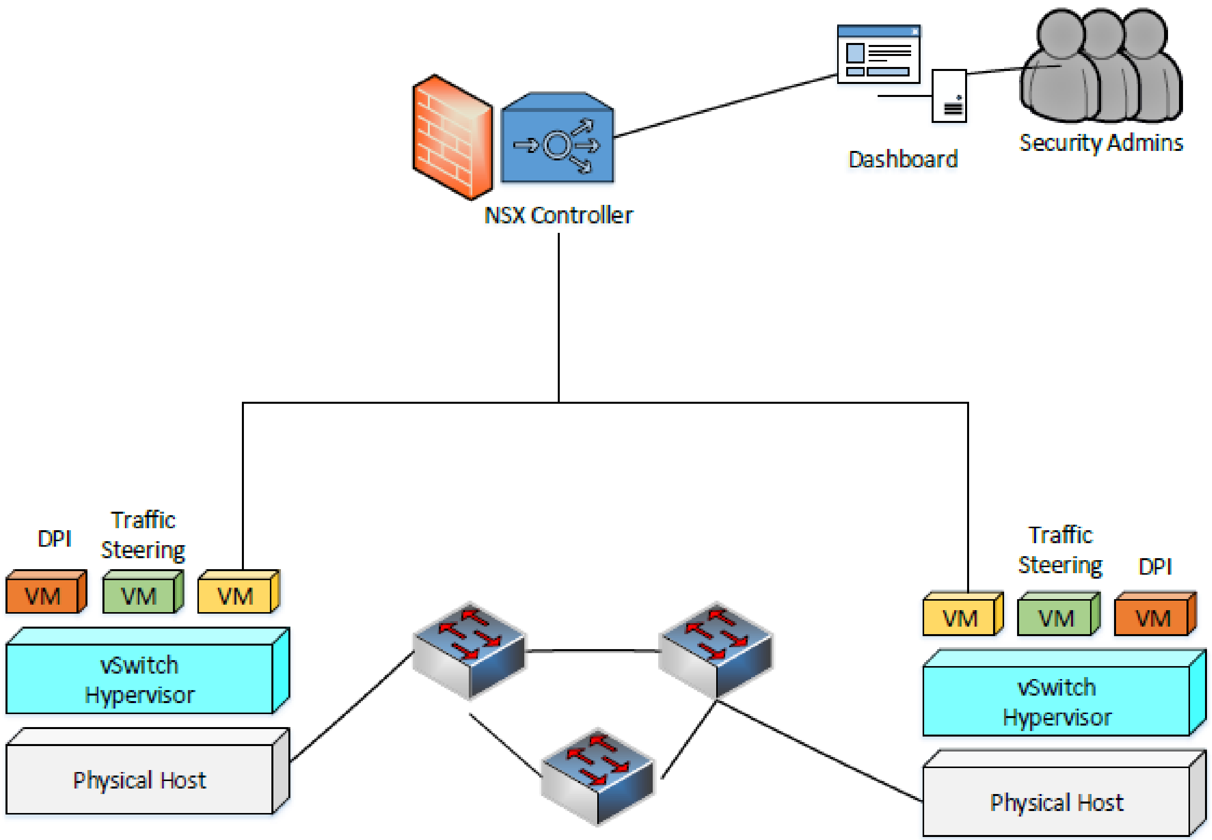
SDN BASED MICRO-SEGMENTATION FOR APT DEFENSE



SDN BASED MICROSEGMENTATION FOR APT DEFENSE

- SDN controller can centrally enforce micro-segmentation policy.
- WEBA can communicate with FEECOM002 and CRMAPP2, similarly, the applications with same colors are allowed to communicate.
- Lateral movement of the attacker is localized only to the infected host/application.
- Distributed Security Framework: Micro-segmentation at network gateway, subnet-level, host-firewall level.

SDN ENABLED SECURED SERVICE FUNCTION CHAINING FOR APT DEFENSE



SDN ENABLED SECURED SERVICE FUNCTION CHAINING FOR APT DEFENSE

- IDS/IPS, Firewall, Data Loss Prevention (DLP) in isolation may limited protection against sophisticated attacks.
- The flow rules at of OpenFlow switches can be modified in order to create a chain of security functions between the source and destination of the network traffic.
- Traffic can be steered through a series of inspection increasing the likelihood of APT attack detection/mitigation.

PROBLEMS IN APPLICATION OF INTELLIGENCE IN CYBERSECURITY

Outlier Detection, High Cost of Errors, Semantic Gap, Variance in Network Traffic

PROBLEMS IN APPLICATION OF INTELLIGENCE IN CYBERSECURITY

- NIDS systems that utilize misuse detection and anomaly detection can suffer from false positives and false negatives.
- Cost of misclassifying the normal user activity such as failed login attempts as abnormal.
- Failure to identify malicious activity correctly can prove to be quite costly.

ISSUES IN APPLICATION OF MACHINE LEARNING FOR NIDS

- High cost of errors.
- Lack of suitable training data;
- Semantic gap between results predicted by ML and their operational interpretation.
- High variation in the input data.

ISSUES IN APPLICATION OF MACHINE LEARNING FOR NIDS

- ML algorithm requires domain expertise and semantic insights into system capabilities.
- Generic problems such as false positive and false negative.
- Cybersecurity domain enhances the probability of errors because adversarial users can try to evade detection.

OUTLIER DETECTION ISSUES

- Classification algorithms utilize collaborative filtering to match users preferences and positive ratings.
- Anomaly detection algorithm, on the other hand, would try to identify an anomalous pair of items.
- Machine Learning training phase would require a large number of samples of both normal as well as abnormal activity, e.g., NIDS logs.

OUTLIER DETECTION ISSUES

- In a real-world setting, most of the traffic is normal.
- ML-based NIDS systems end up training the detection algorithm on only one class of training samples.
- Closed world assumption that any test sample not matching the feature set of normal traffic is anomalous is not practical.

HIGH COST OF ERRORS

- False positive in the case of a network intrusion event can lead to loss of service.
- Waste significant man-hours for an analyst who is responsible for analyzing the intrusion activity.
- Event few false positives can render the NIDS useless.
- False negatives can, on the other hand, disrupt the security of the organization significantly.

SEMANTIC GAP ISSUE

- Semantic Gap: Output of NIDS and the semantic vs meaning of the reports from the network operators point of view.
- For a production-grade NIDS, the semantic gap issue should be addressed.
- Local security policies, site-specific properties should be identified incorporated in definition of malicious vs benign activity.
- E.g. – P2P traffic is considered normal as part of site-specific properties in a network, whereas the absence of this information can traffic being flagged as malicious.

VARIANCE IN NETWORK TRAFFIC

- Network traffic bandwidth, latency, network protocols can show significant variation even within the same network environment.
- Data transfer between applications within the same environment can show a spike in network traffic.
- Anomaly detection system can find such variability difficult to interpret.
- Operational knowledge of the network is required in such cases

CITE THIS WORK

```
@book{huang2018software,
title={Software-Defined Networking and Security: From Theory to Practice},
author={Huang, Dijiang and Chowdhary, Ankur and Pisharody, Sandeep},
year={2018},
publisher={CRC Press}}
```

REFERENCES

- https://thehackernews.com/2016/04/artificial-intelligence-cyber-security.html
- https://people.csail.mit.edu/kalyan/AI2_Paper.pdf
- https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2010/in-depth_analysis_of_hydraq_final_231538.pdf
- https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf