Web Shell Attack

Dr. BhawanaRudra
Assistant Professor
Department of Information Technology
National Institute of Technology Karnataka

Definition

- A WebShell is a piece of code or a script running on a server that enables remote administration. While often used for legitimate administration purposes, it is also a favorite tactic used by malicious actors in order to gain remote control of internet-facing web servers.
- Once interaction with a WebShell is established, an attacker is free to act on any number of objectives such as service disruption, increasing foothold, and data exfiltration
- Webshell is a web vulnerability and a security threat to any user or a server that can be accessed by attackers to control our system.

Cyber threats and concerns

International level

- Cyber crime & cyber terrorism
- Deliberate and anonymous use of ICTs for attacks on critical Infrastructure
- Unhindered growth of botnets
- Absence of international mechanism to facilitate information sharing & counter action
- Risk of attack misperception due to uncertainty of positive attack attribution

National level

- Cyber crime & terrorism
- Attacks on Critical Infrastructure
- Web defacements
- Website intrusion and malware propagation
- Malicious Code & spread of botnets
- Scanning and probing for Cyber espionage
- Denial of Service & Distributed Denial of Service attacks
- Supply chain integrity
- Technical & legal inability for positive attack attribution

Organisational level

- Website intrusion/ defacement
- Domain stalking
- Malicious Code
- Scanning and probing
- Denial of Service & Distributed Denial of Service
- Targeted attacks
- Phishing
- Data theft
- Insider threats
- Financial frauds

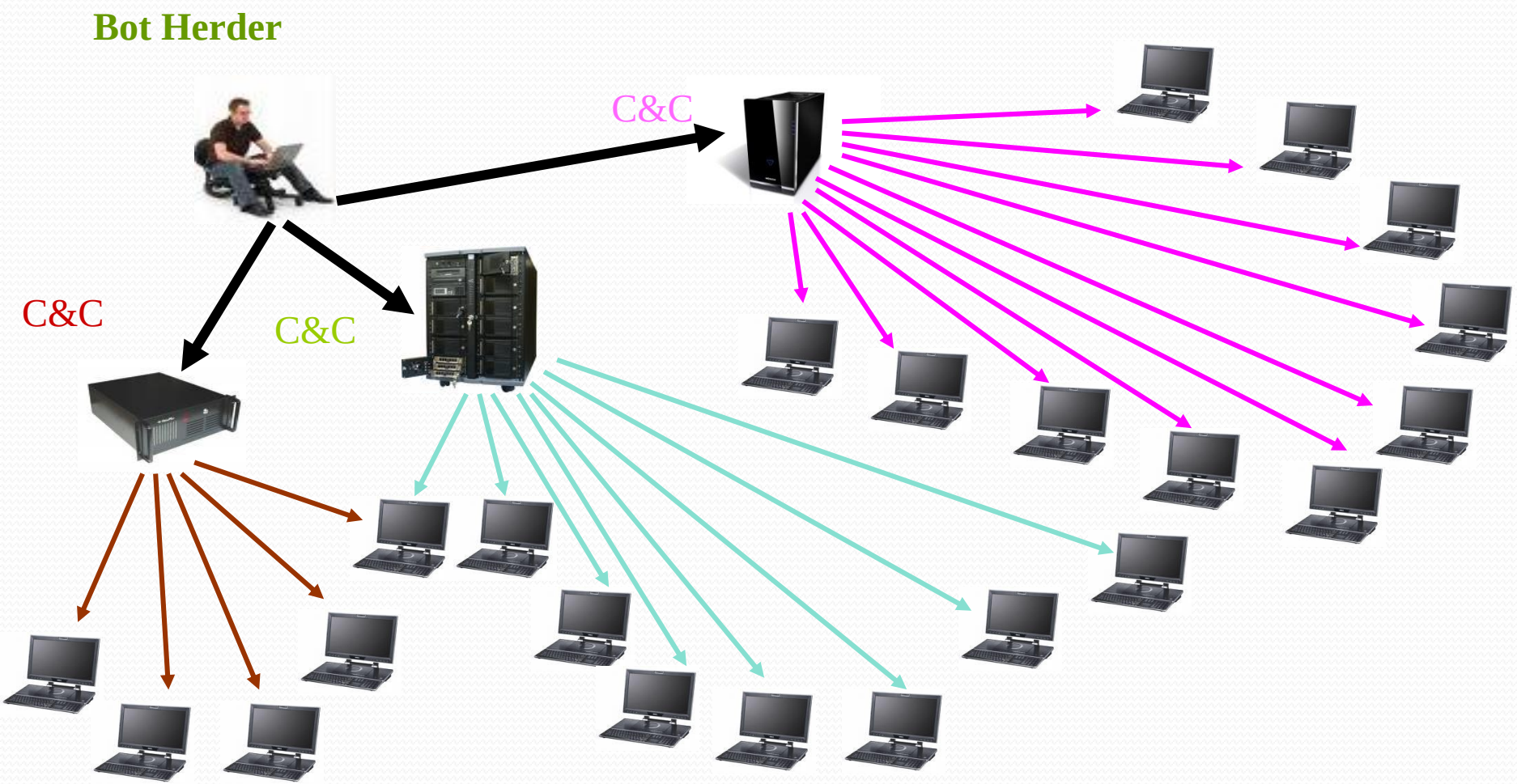
Individual level

- Social Engineering
- Email hacking & misuse
- Identity theft & phishing
- Financial scams
- Abuse through emails
- Abuse through Social Networking sites
- Laptop theft

Disaster Induced by Cyber Attacks

- Attacks on Critical Sector Infrastructure- Nuclear, Power, Defense…
- What will happen, if motor shaft will spin with 100 X of its normal speed?
- What will happen, if control rod of nuclear reactor is controlled by attacker?

C2 Operations and Threats



Lack of Cyber Hygiene - Attack on client side software

- PDF Reader/ Flash
- Microsoft office Docs
- JAVA
- Client side web browsers and extensions /plugins

Web-Application Attacks

- Low-hanging Fruit – In-house developed- **Develop your website just Rs. 500/-**.
- My Valid Email-id

echo 6173686f6f2e6f6e6c696e6540676d61696c2e636f6d | perl -pe 's/(..)/chr(hex($1))/ge'

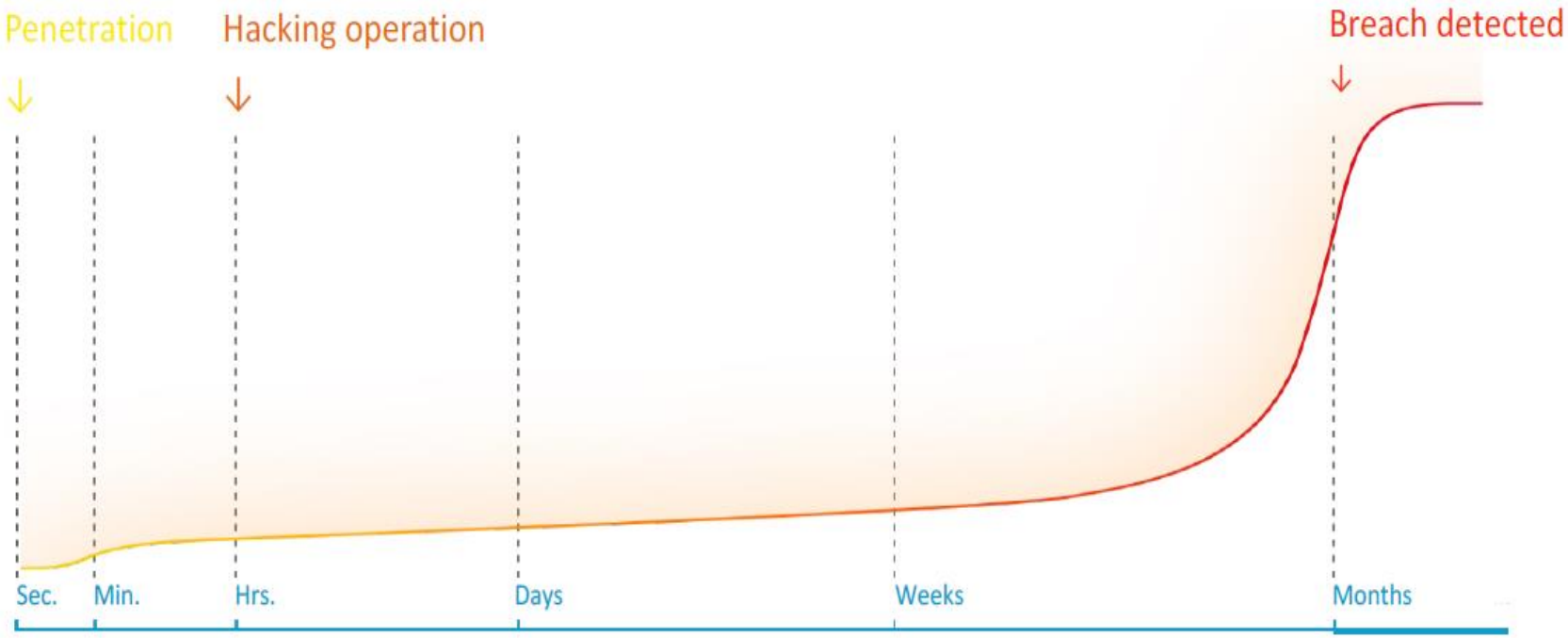
- “75% of all attacks occurring at application layer”—Gartner
- “8 out of 10 websites are vulnerable to attack”—WhiteHat Security Team
- Web apps account for 80% of internet vulnerabilities

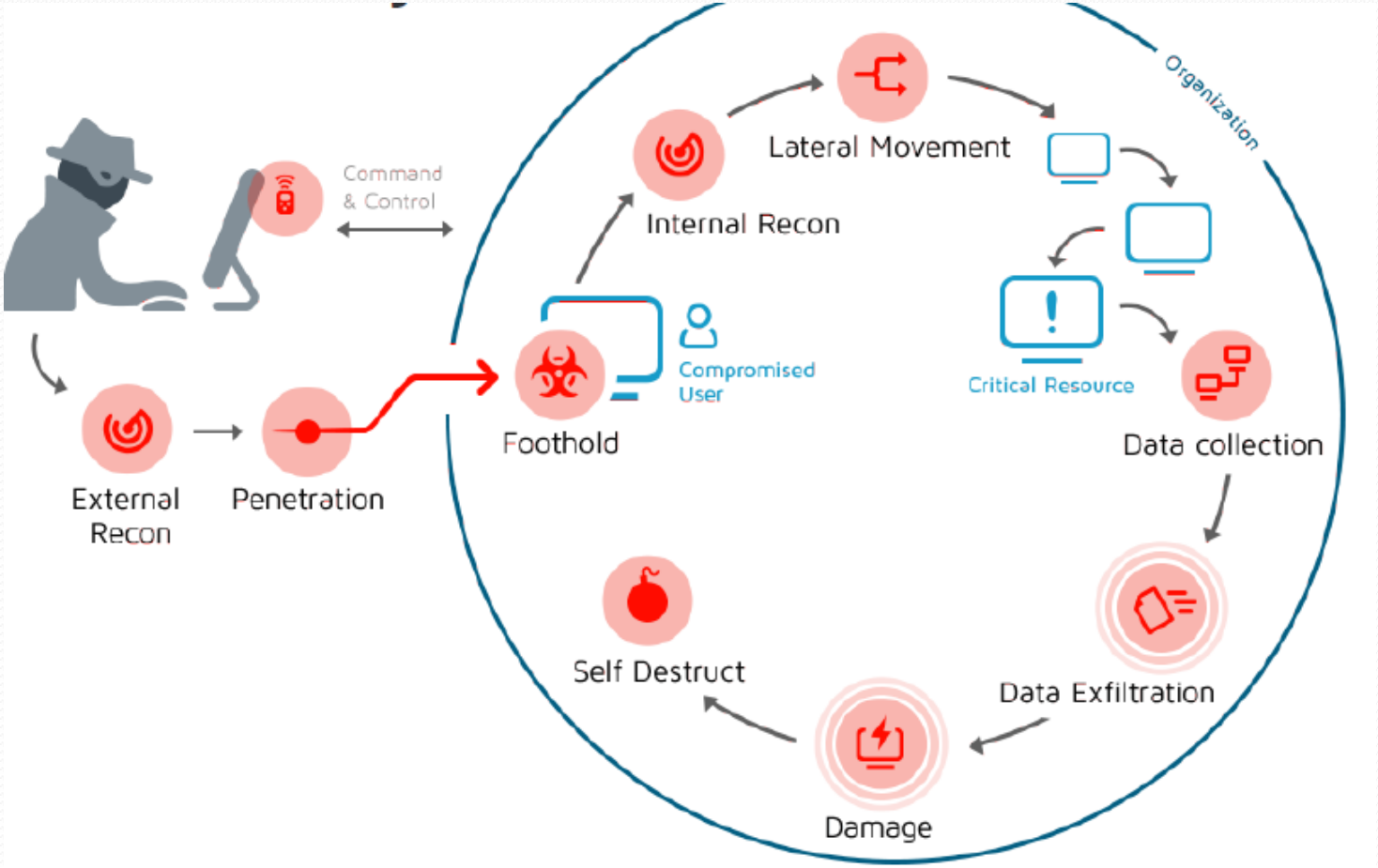
Attacks

- Cross Site Scripting (XSS)
- SQL Injection
- Cross Site Request Forgery (XSRF)
- Malicious File Upload
- Remote File Inclusion (RFI)
- Command Injection

….& more

The Attack (Full) Lifecycle




Command
& Control
External
Recon
Penetration
Foothold
Compromised
User
Internal Recon
Lateral Movement
Organization
Critical Resource
Data collection
Data Exfiltration
Damage
Self Destruct

External Recon

- Social Networking
- Conferences
- Call Help Desk or Admin
- External Scans
- Buy Information/Tools in Black Market

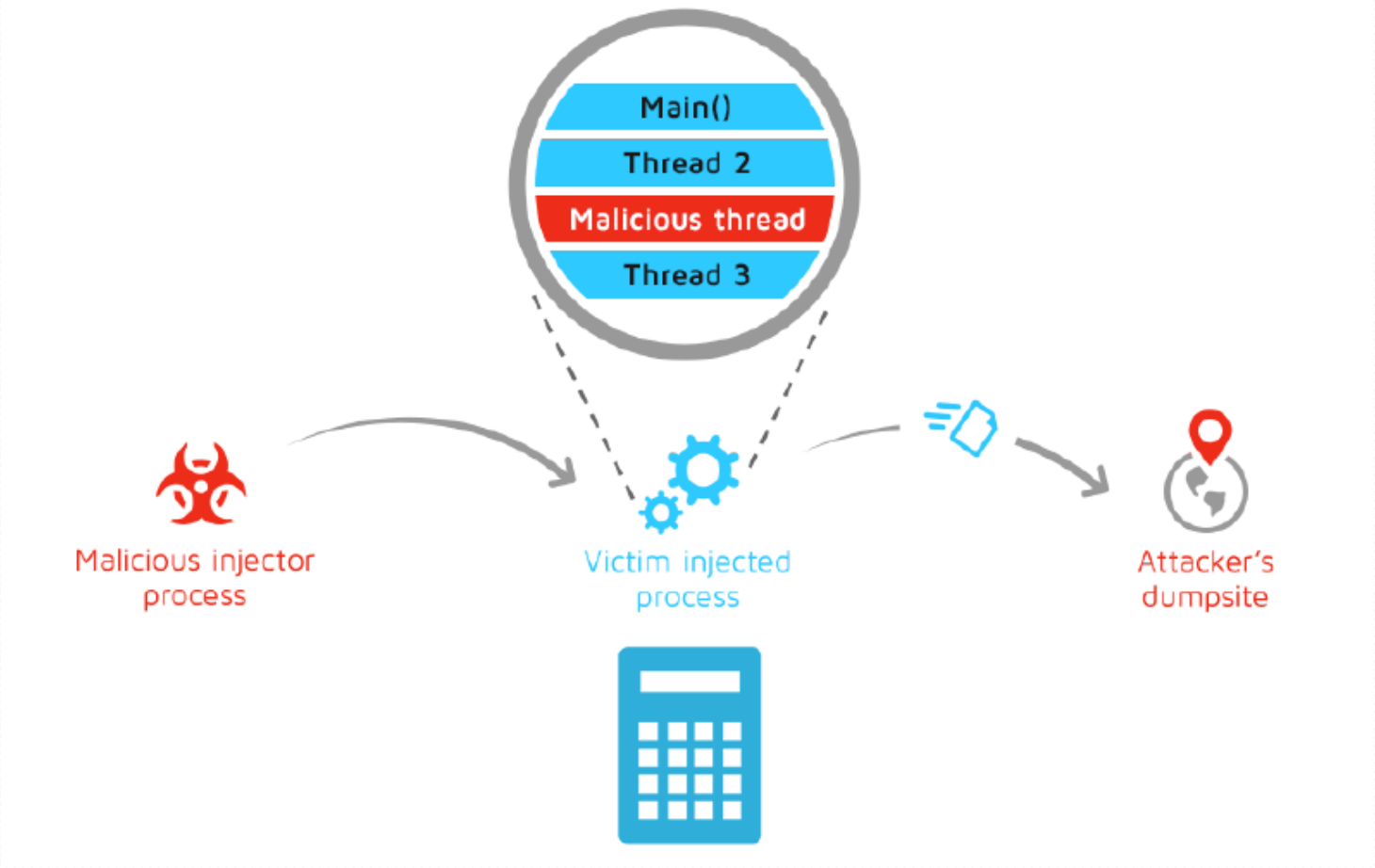
Breach: Penetration. Privilege escalation. Obfuscation.

- Phishing & spear phishing
- Vulnerability exploit
- Social Engineering
- Infected USB drive
- Compromised credentials
- Autorun
- Process Injection

Process Injection

Running another procedure as a thread inside another process.

- Evasion
- Reading host process memory
- Affecting host process behavior


Main()
Thread 2
Malicious thread
Thread 3
Malicious injector process
Victim injected process
Attacker's dumpsite

Command & Control

Operation. Exfiltration.

- Legitimate HTTP
- Legitimate DNS request
- Fust Flux
- TOR
- Facebook / Twitter / YouTube comments
- Domain Generation Algorithm

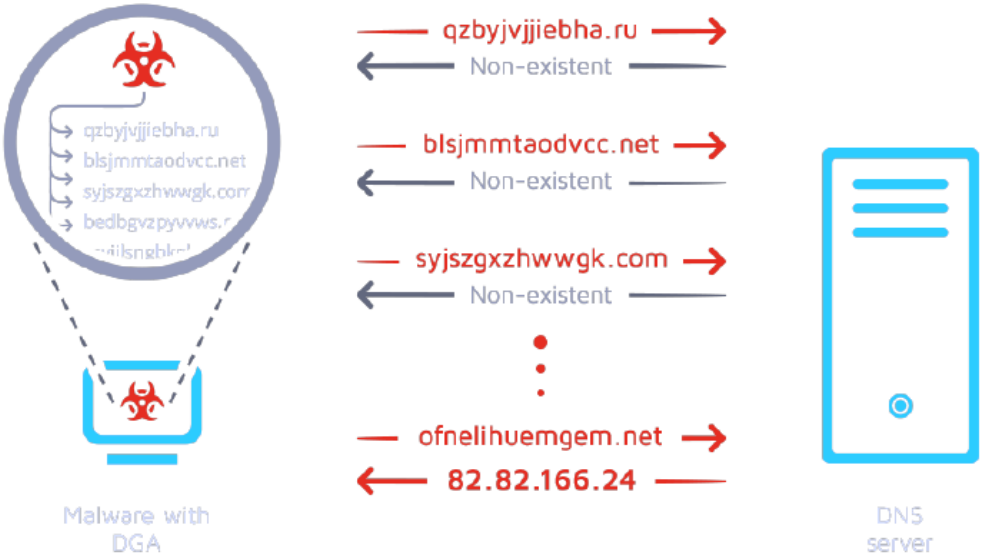
Command & Control

Domain generation algorithm

- Regular C&C servers can be blacklisted and firewalled
- DGA is generating a daily domain list (1000's of domains)
- Malware tries to resolve each one of those random domains.
- The attack (who created the algorithm) knows which domains will be generated.
- Once a certain C&C domain is blocked, attacker can select one of the daily generated domains, register it and continue his endeavors.

Command & Control

DGA

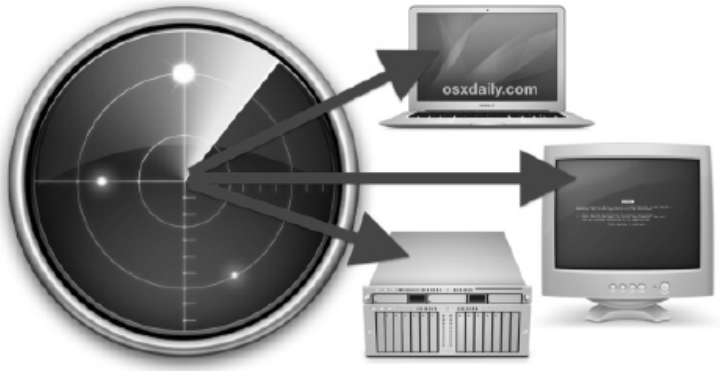


Breach | C & C | Recon | Spread | Damage

Recon

Scanning

- ARP scanning
- SYN scanning
  - ("half-open scanning“)
- FYN scanning
- Port scanning

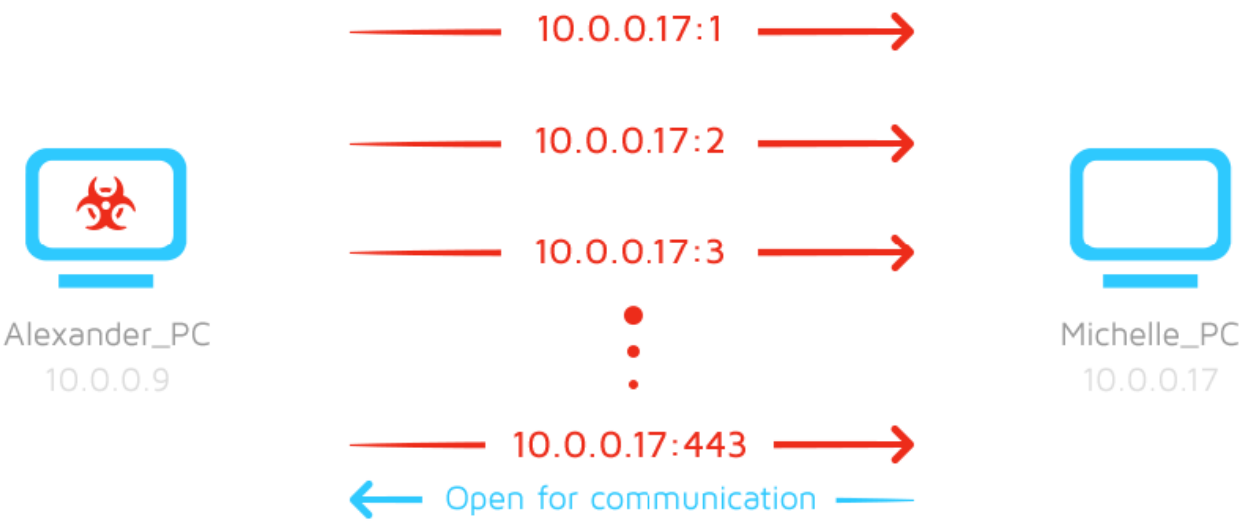


Reconnaissance
Port Scanning

- Services are using ports to communicate (HTTP = 80, DNS = 53, etc.)
- When an attacker gets a foothold on a computer, he needs to move around the organization.
- The attacker scans the subnet to find exposed and exploitable services on other computers and platforms.
- Once an open port is found, further exploitation occurs.

Reconnaissance

Port Scanning



Spread

Lateral movement - Legitimate tools used maliciously.

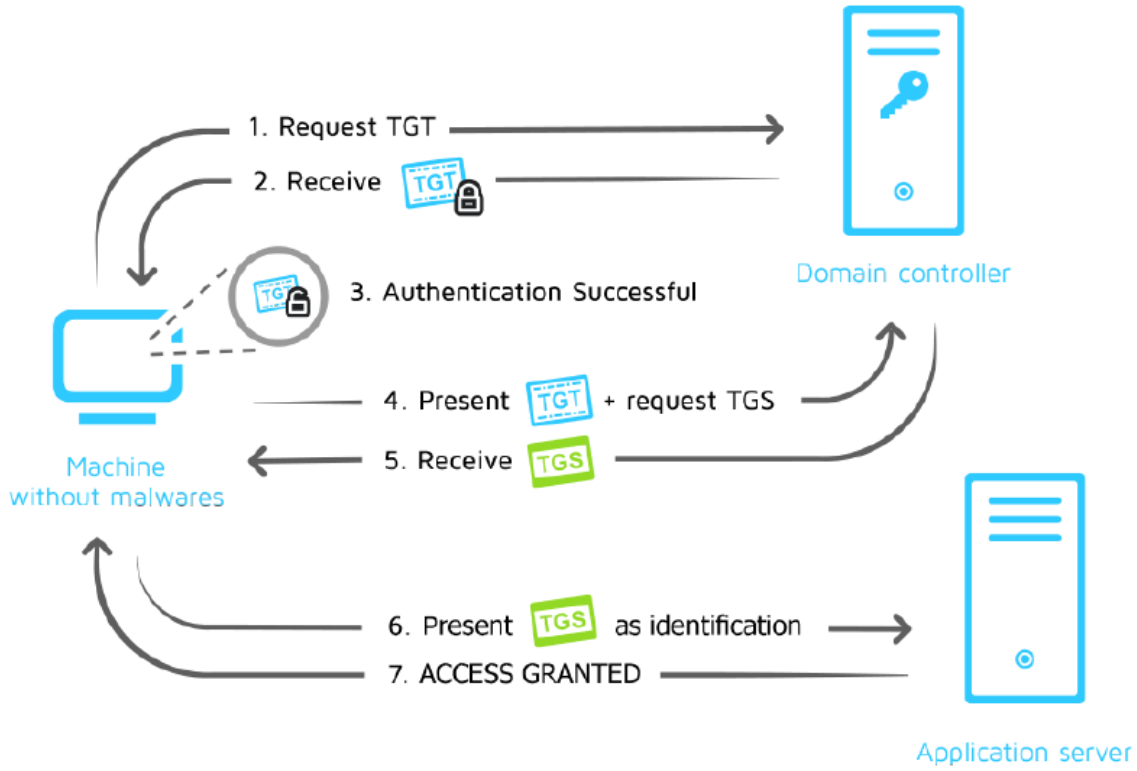
- Pass The Hash/Ticket
- Shares
- PSExec

Spread

PSEXEC - Legitimate tools used maliciously.

- A legitimate tool by Microsoft.
- Commonly used by IT professionals
- Allows to run a process on a remote machine interactively.
- Attackers use that technique to spread their malware through an entire network.

Lateral Movement --- Pass-the-ticket



Damage. Business. Money. Physical.

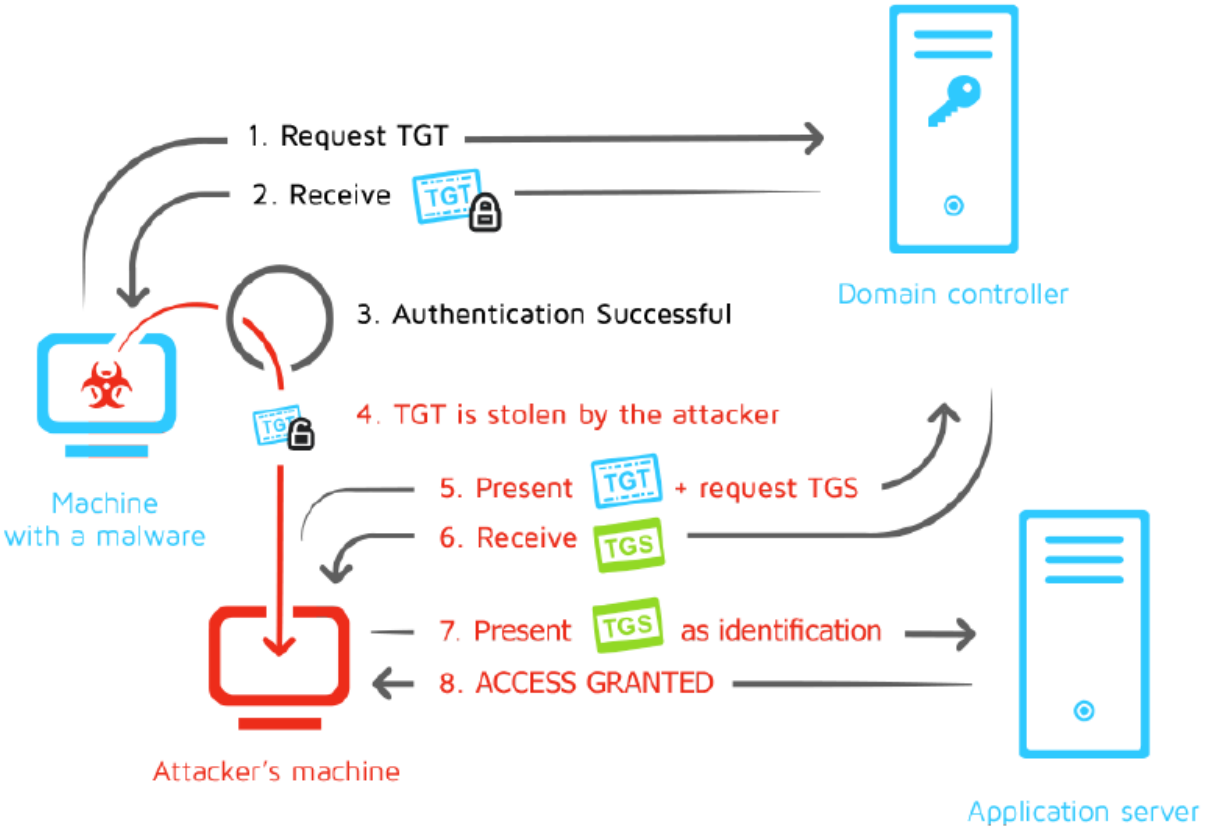
Cyberattack on German steel factory causes 'massive damage'

BUSINESS

Home Depot's 56 Million Card Breach Bigger Than Target's

'Unique, Custom-Built Malware' Eliminated From Retailer's Systems After Five-Month Attack on Terminals

Lateral Movement --- Pass-the-ticket



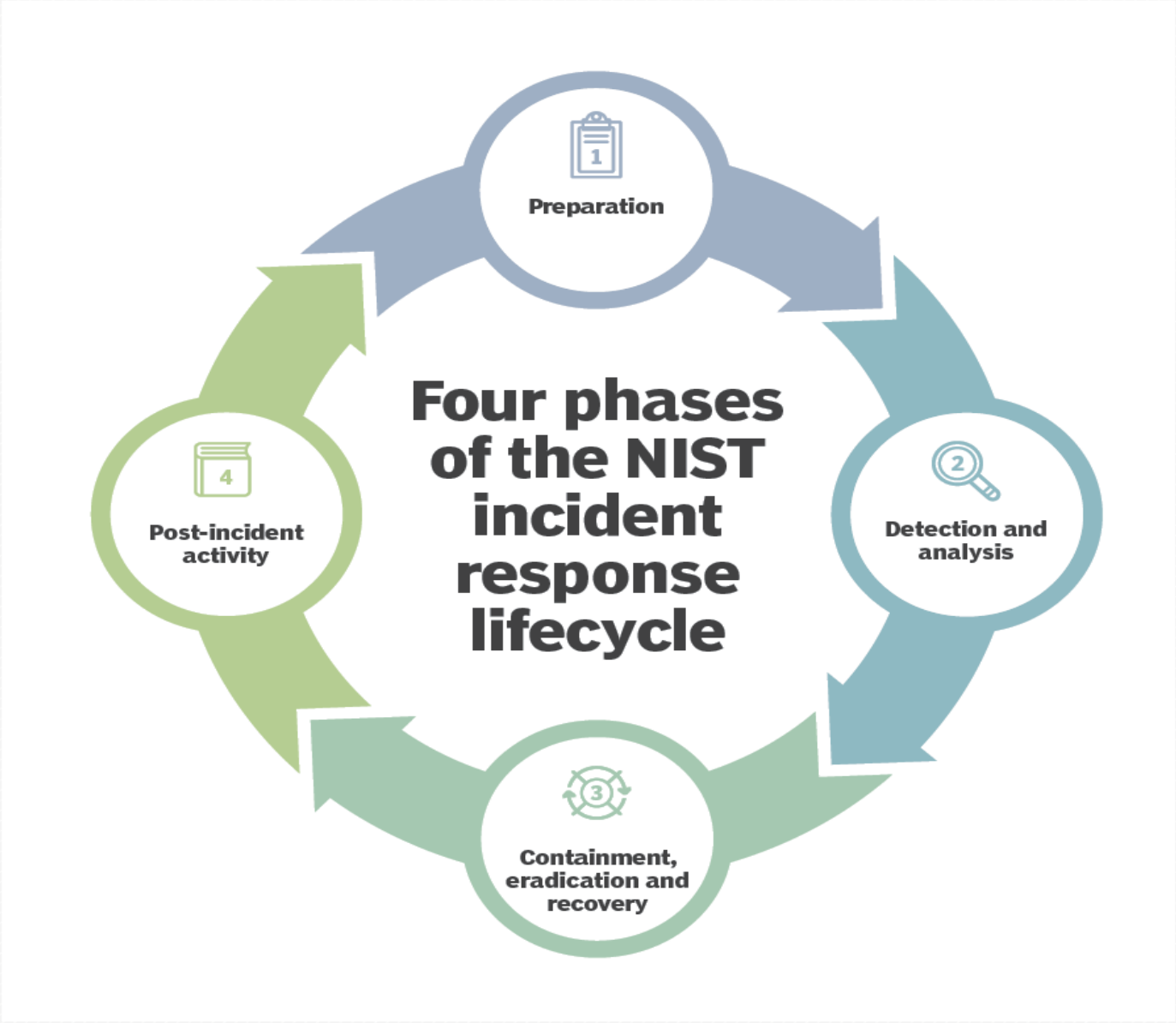
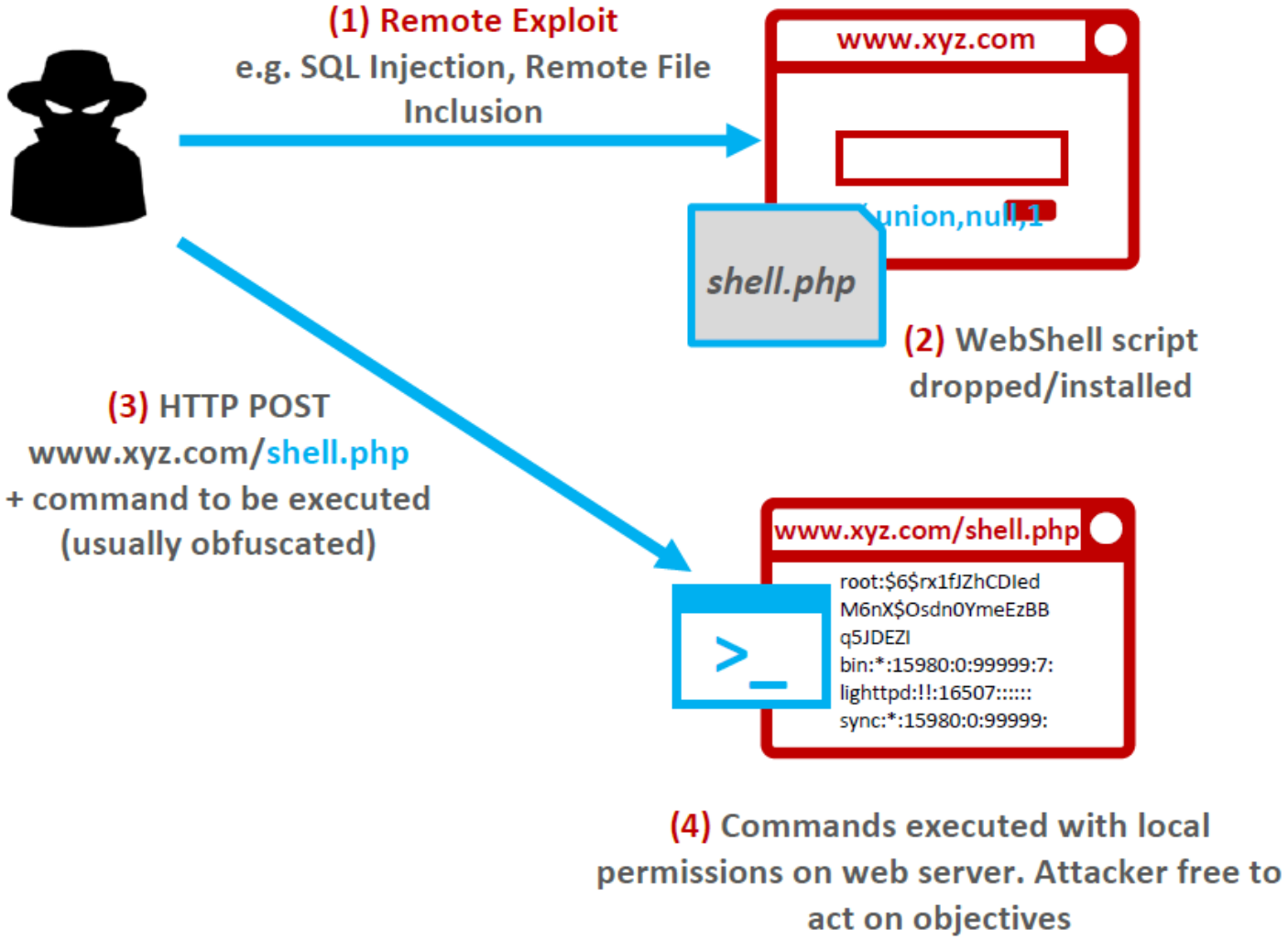
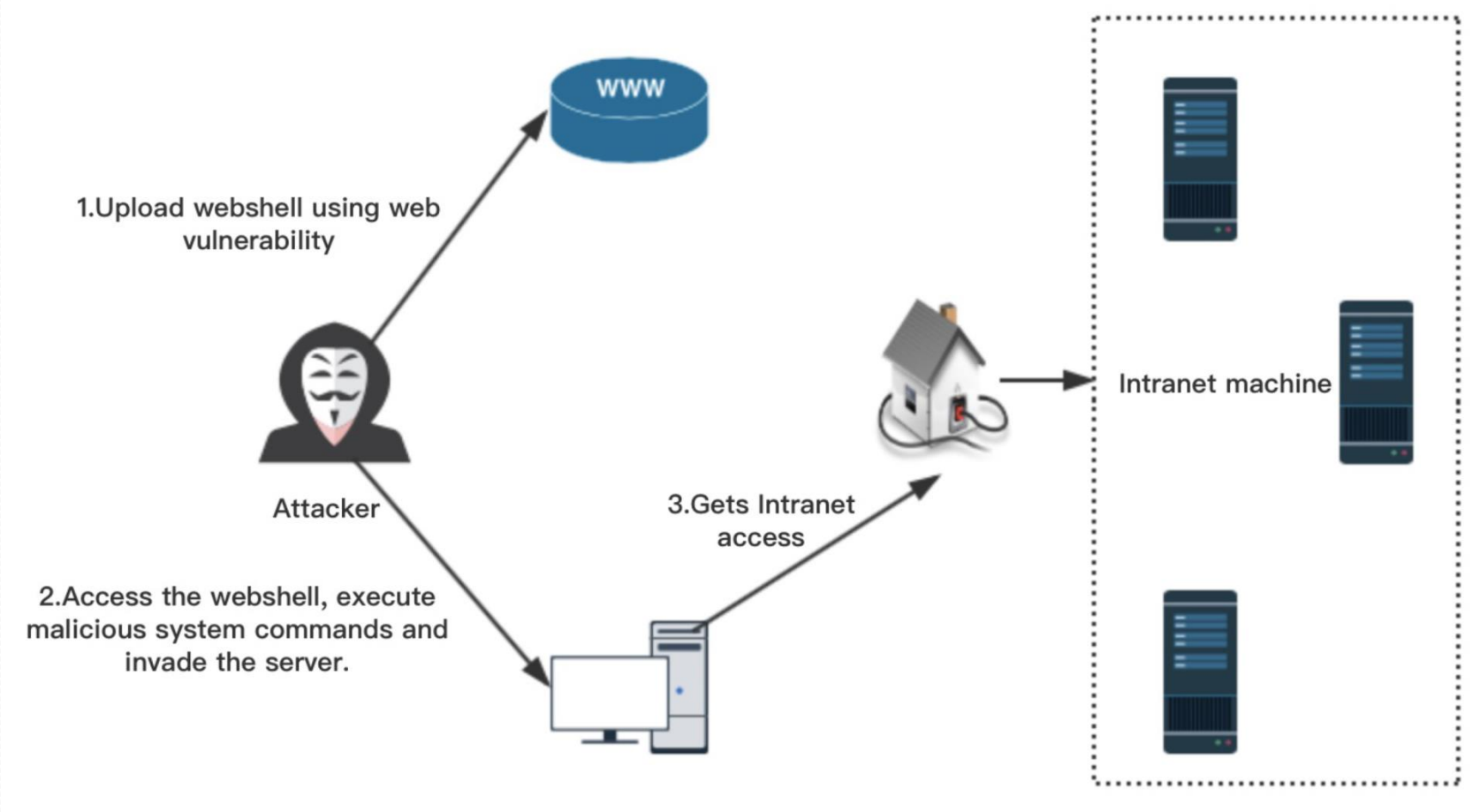


ILLUSTRATION: ALEXDNDZ/ADOBE STOCK; FIREOFHEART/GETTY IMAGES


(1) Remote Exploit
e.g. SQL Injection, Remote File Inclusion
www.xyz.com
union,null,1
shell.php
(2) WebShell script dropped/installed
(3) HTTP POST
www.xyz.com/shell.php
+ command to be executed
(usually obfuscated)
www.xyz.com/shell.php
root:6rx1fJZhCDIed
M6nX$Osdn0YmeEzBB
q5JDEZI
bin:*:15980:0:99999:7:
lighttpd:!!:16507::::::
sync:*:15980:0:99999:
(4) Commands executed with local permissions on web server. Attacker free to act on objectives

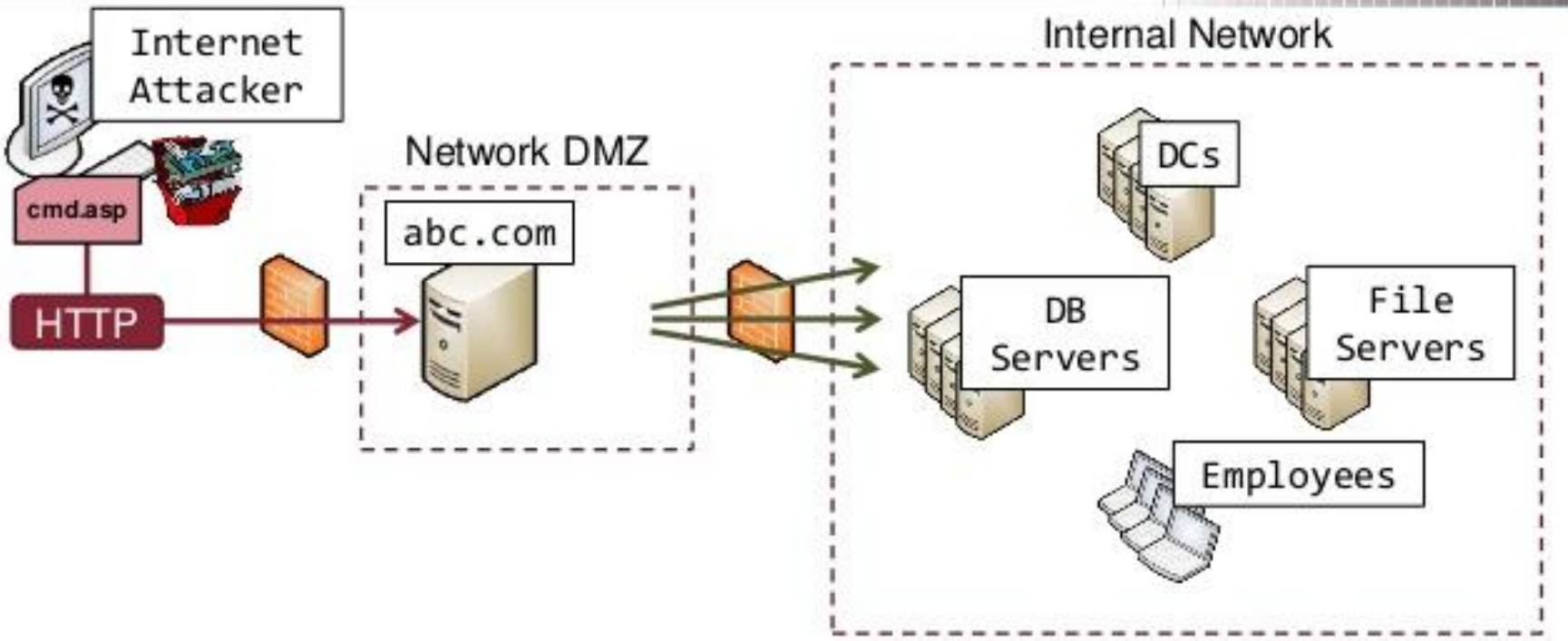

WWW
1.Upload webshell using web vulnerability
Attacker
2.Access the webshell, execute malicious system commands and invade the server.
3.Gets Intranet access
Intranet machine

	Delivery SQL Injection RFI Other Web Exploit	**Exploit/Installation** Creation/installation of WebShell script on web server	**C2** Obfuscated commands via HTTP POST	**Action** Data Exfiltration Lateral Movement Disruption
AV/FW/IDS/IPS:				
Traditional SIEM:				
RSA NetWitness Logs and Packets:				

No visibility	**Partial Visibility/Signature**	**Full Visibility**

Classic Web Shell Attacks

MANDIANT



Attacker uploads a malicious dynamic web page to a vulnerable web server

Attacker uses the "web shell" to browse files, upload tools, and run commands

Attacker escalates privileges and pivots to additional targets as allowed


Define
Diagram
Identify
Mitigate
Validate
Threat
Modeling