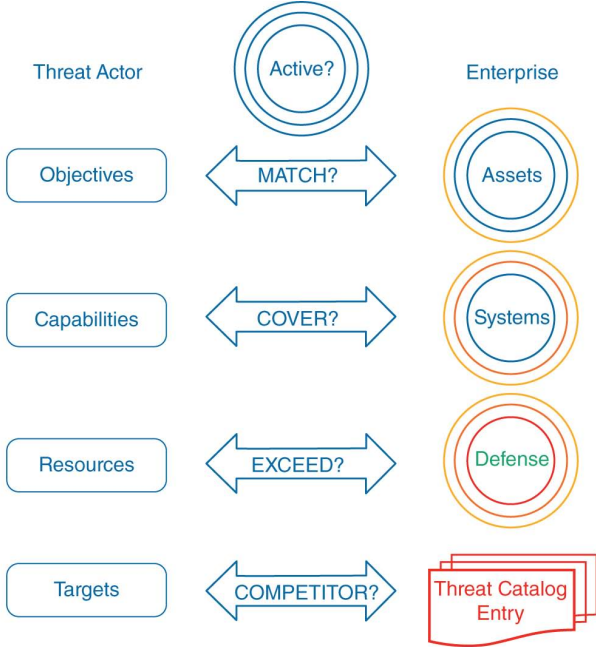


Threat Actor Type	Objective
Activist/Hacktivist	Make a political statement (Anonymous); voting systems
Competitor	Trade secrets, competitive analysis, or disruption of service
Criminal	Profit; anything they can monetize for cash
Crime-syndicate	Organized crime as a technology business
Hacker	Hacking for thrill or challenge
Insider-accidental	Unintentionally exposes the organization to harm
Insider-disgruntled	Financial gain; personal benefits for retaliation or revenge
Nation-state	World supremacy
Sensationalist	Embarrassment and brand damage
Spy	Cyber espionage
Terrorist	Telecom, energy grid, government defenses
Other, e.g. Lone Wolf	Cybercrime-as-a-service model is furthering the reach of solo actors.

Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 2.3



Example Courtesy of FrameCyber®

ID: **CP** Threat Type: **Activist** Threat Role: **Director** Threat Level: **Intermediate**

Name: **Cyber Partisans** Geolocation: **Belarusian Diaspora** Aliases:

Description:

Cyber Partisans, is a group advocating for Belarusian civil rights, many of whom are Belarusian refugees. Other than a New York spokesperson, their location is not known and identities remain anonymous even to each other. The group describes its activities as ethical hacking, as it only attacks the state and does no harm to ordinary citizens.

Tactics:

The group has selected two types of targets: those that have sensitive information that can assist opponents of the Belarus regime and those that disrupt or disable critical infrastructure. For example, they hacked the Ministry of Internal Affairs most sensitive

Skills:

Member skills included the development of malicious software, penetration testing, and data science.

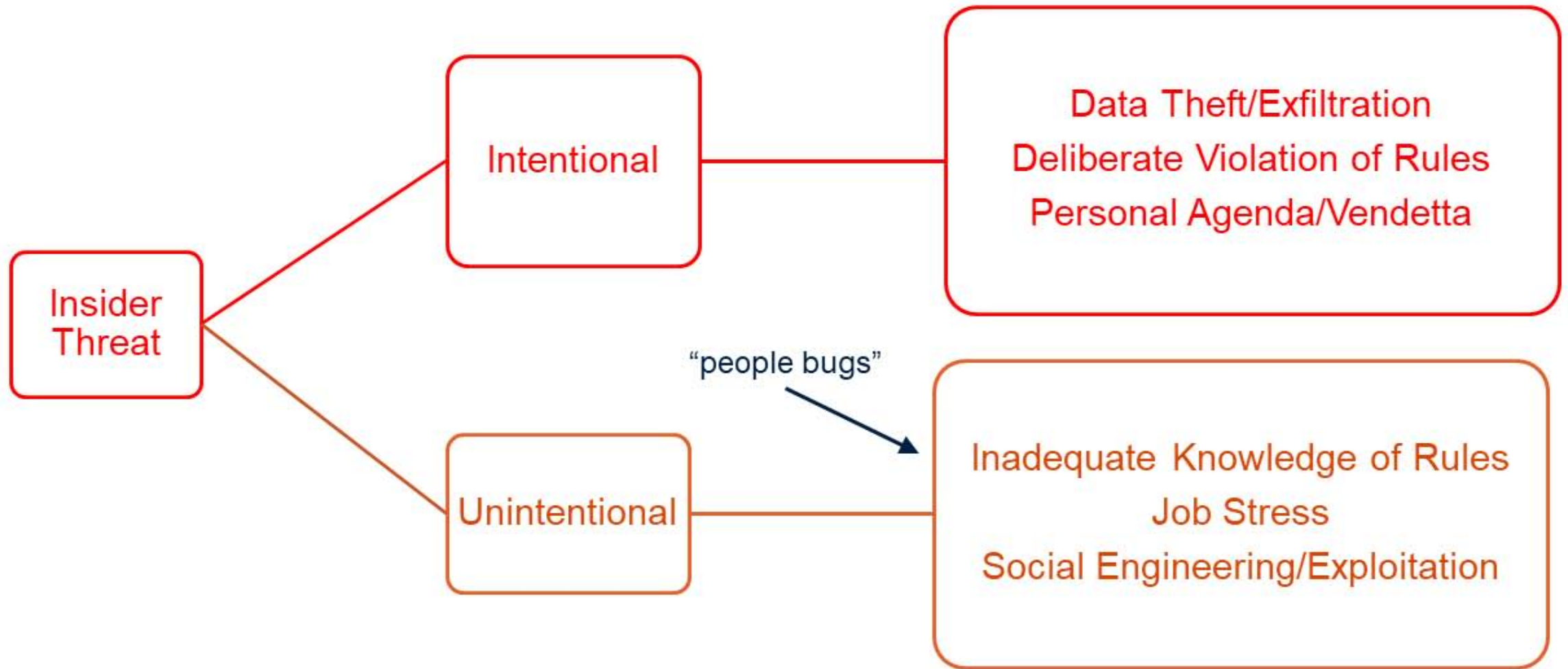
Goals:

Expose the crimes of the Belarus government and stop violence and repression from the regime and restore democracy and rule of law.

Resources:

CP consists of a group of ~50 people assisted by former Belarusian police officers who understand government data structures.

Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 2.5



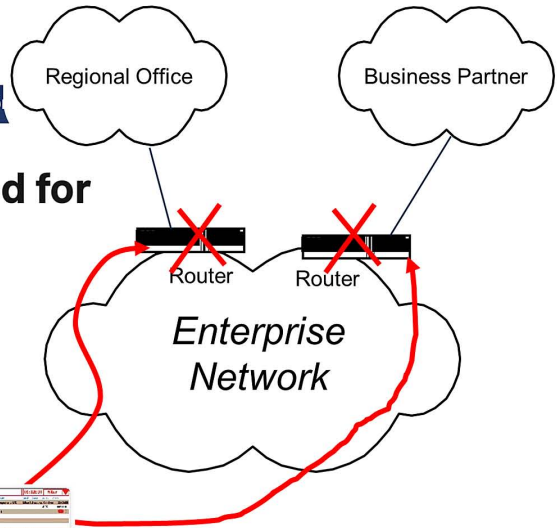
DALLAS

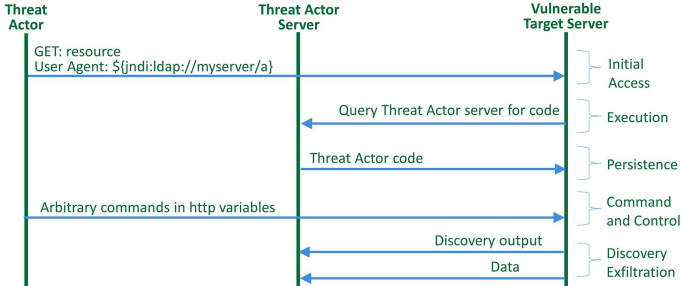
Dallas Citibank Worker Sentenced for Computer Sabotage

Published July 26, 2016 • Updated on July 26, 2016 at 9:15 am

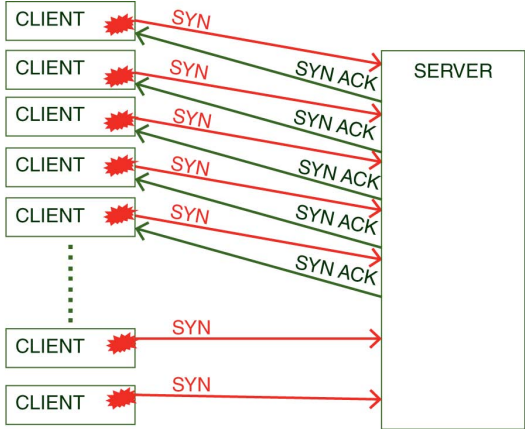
An employee who sabotaged Citibank's computer system because he believed he was about to be fired was sentenced to nearly two years in prison.

Investigators said Lennon Ray Brown of Dallas transmitted a code and command in 2013 leading to loss of connectivity to 90 percent of Citibank networks in North America.





Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 2.8



```
login = username_field_contents
```

```
pwd = password_field_contents
```

```
user_data = select user from CustomerData where (user.name = login) and (user.password = pwd)
```

```
display user_data
```

USERNAME:

JDOE

JDOE or 'TRUE = TRUE'

PASSWORD:

3yp@3iVS=q

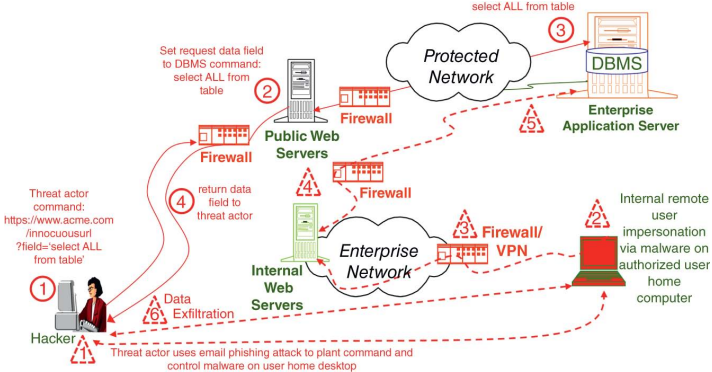
JDOE or 'TRUE = TRUE'

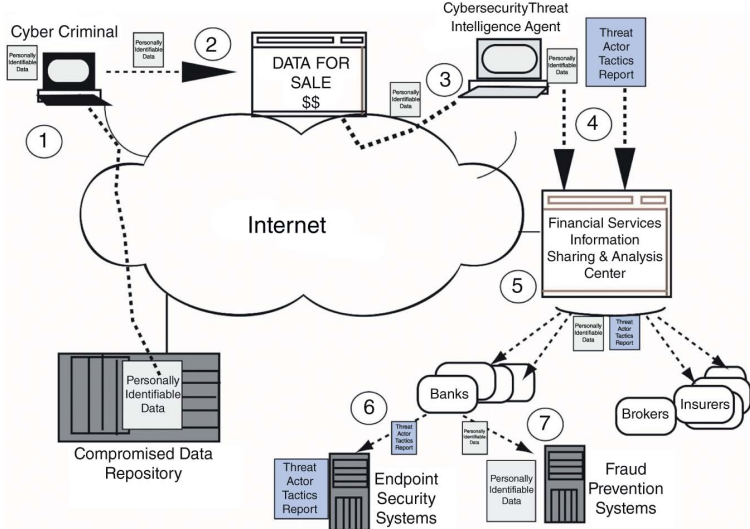


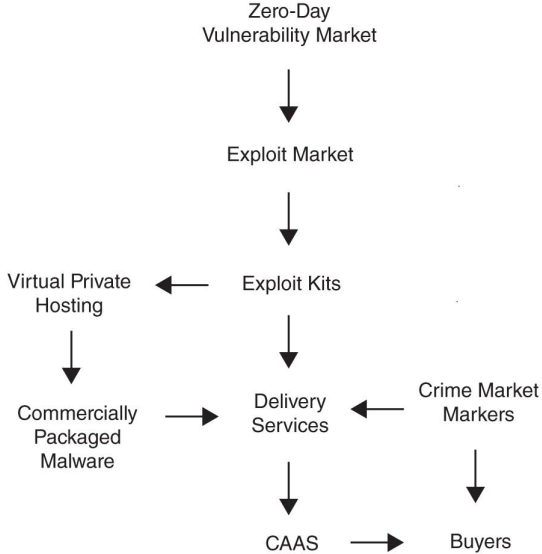
JDOE's data



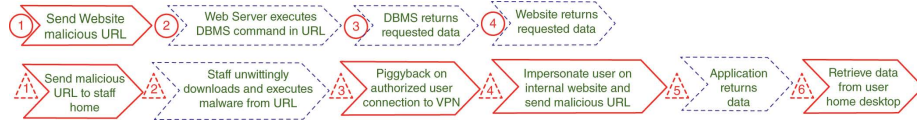
All user data







Reconnaissance	Gather information to plan future operations.
Resource Development	Establish resources to support operations.
Initial Access	Access target system or network.
Execution	Run malicious code on target system.
Persistence	Maintain a foothold within target systems.
Privilege Escalation	Gain higher-level permissions.
Defense Evasion	Avoid being detected.
Credential Access	Steal account names and passwords.
Discovery	Map out target environment.
Lateral Movement	Move through target environment.
Collection	Gather data of interest to goal.
Command and Control	Communicate with compromised systems to control them.
Exfiltration	Steal data.
Impact	Manipulate, interrupt, or destroy target systems and data.

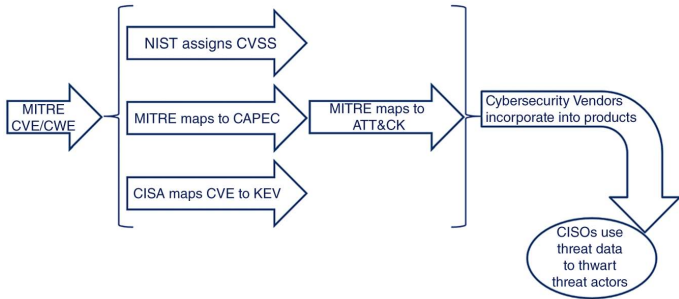


Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 2.15

Table 1 - Vulnerability Tower of Babel, 1998

Organization	Name referring to vulnerability
AXENT (now Symantec)	phf CGI allows remote command execution
BindView	#107—cgi-phf
Bugtraq	PHF Attacks—fun and games for the whole family
CERIAS	http_escshellcmd
CERT	CA-96.06.cgi_example_code
Cisco Systems	HTTP—cgi-phf
CyberSafe	Network: HTTP ‘phf’ attack
DARPA	0x00000025 = HTTP PHF attack
IBM ERS	ERS-SVA-E01-1996:002.1
ISS	http—cgi-phf
Symantec	#180 HTTP server CGI example code compromises http server
SecurityFocus	#629—phf Remote Command Execution Vulnerability

Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 2.16



Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 2.17

Initial Access → Execution → Persistence → Escalation → Evasion → Access → Discovery → Movement → Data → Commands → Exfiltration

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

Legend

- High Confidence of Detection
- Some Confidence of Detection
- Low Confidence of Detection

© 2023 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation, see <https://attack.mitre.org/matrices/enterprise/>

Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 2.18