



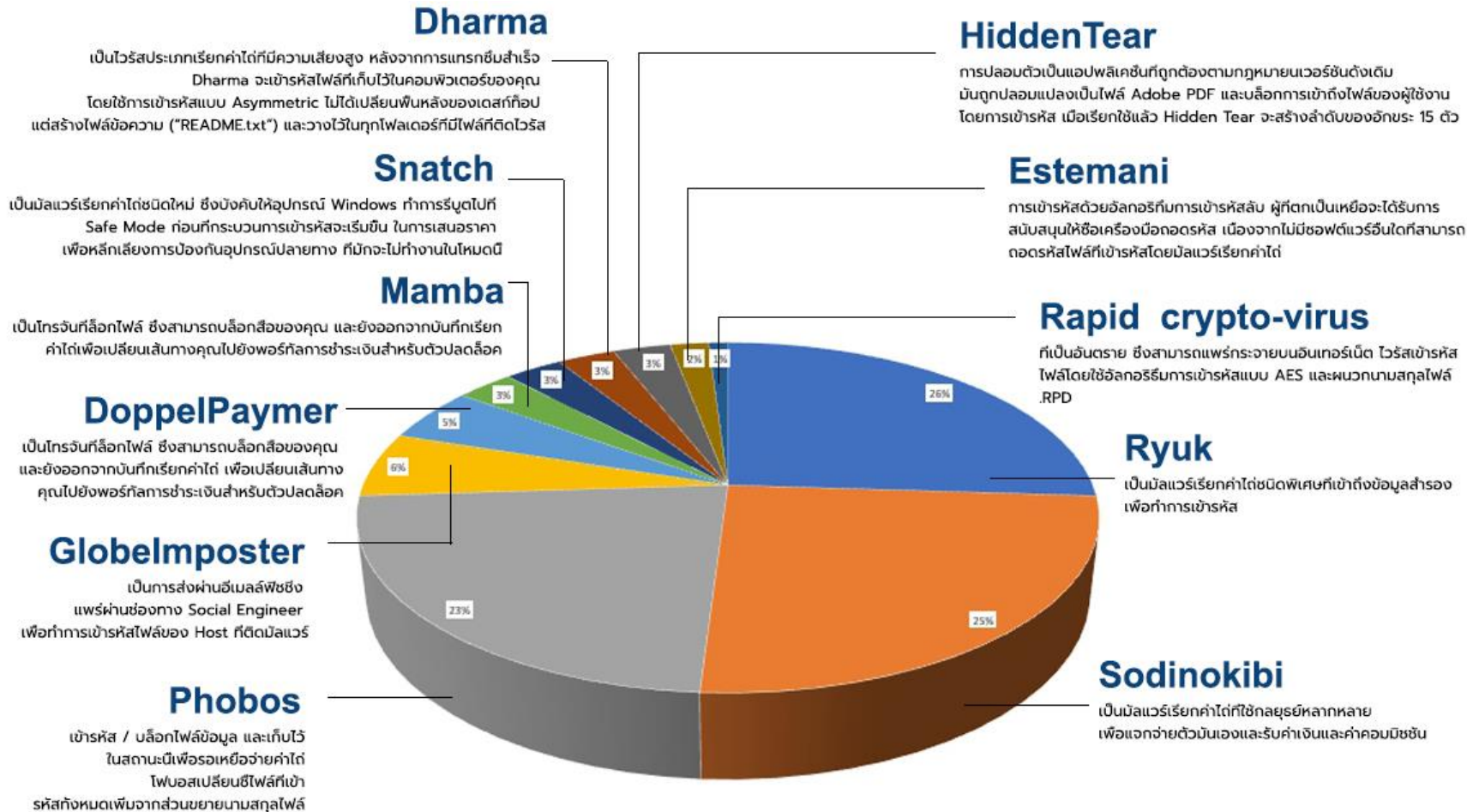
CYBERSECURITY KNOWLEDGE SHARING #2

“Cybersecurity Risks :
Ransomware Awareness”

Section III

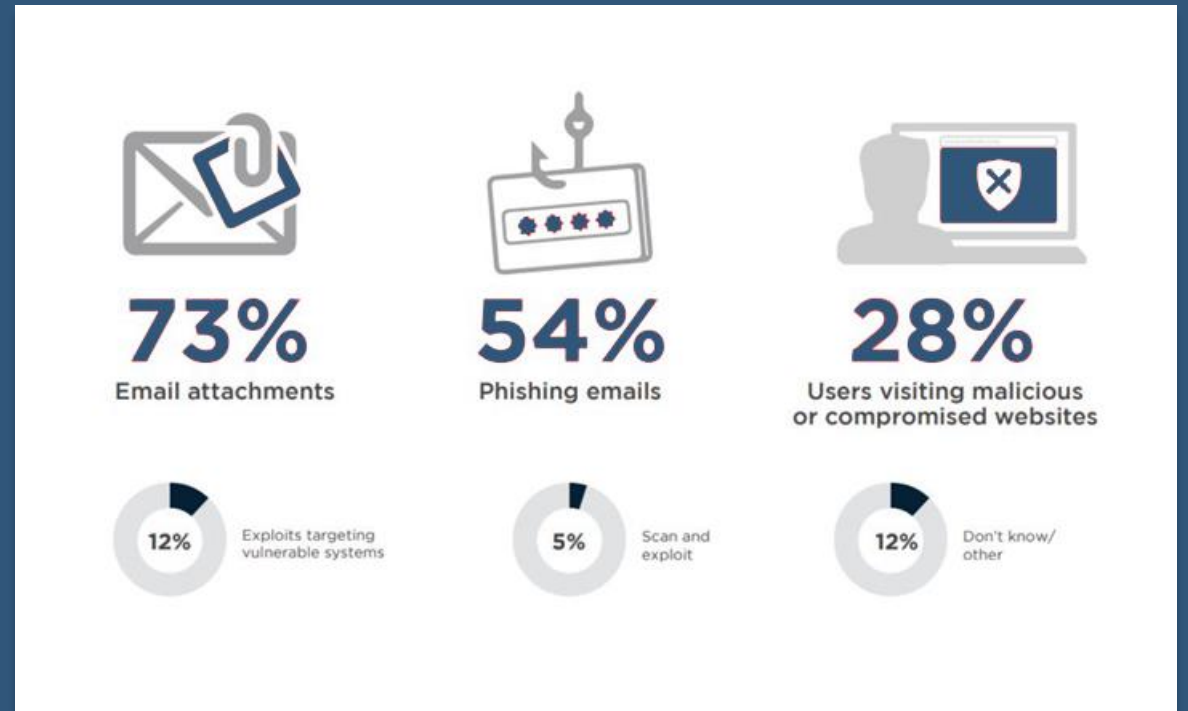
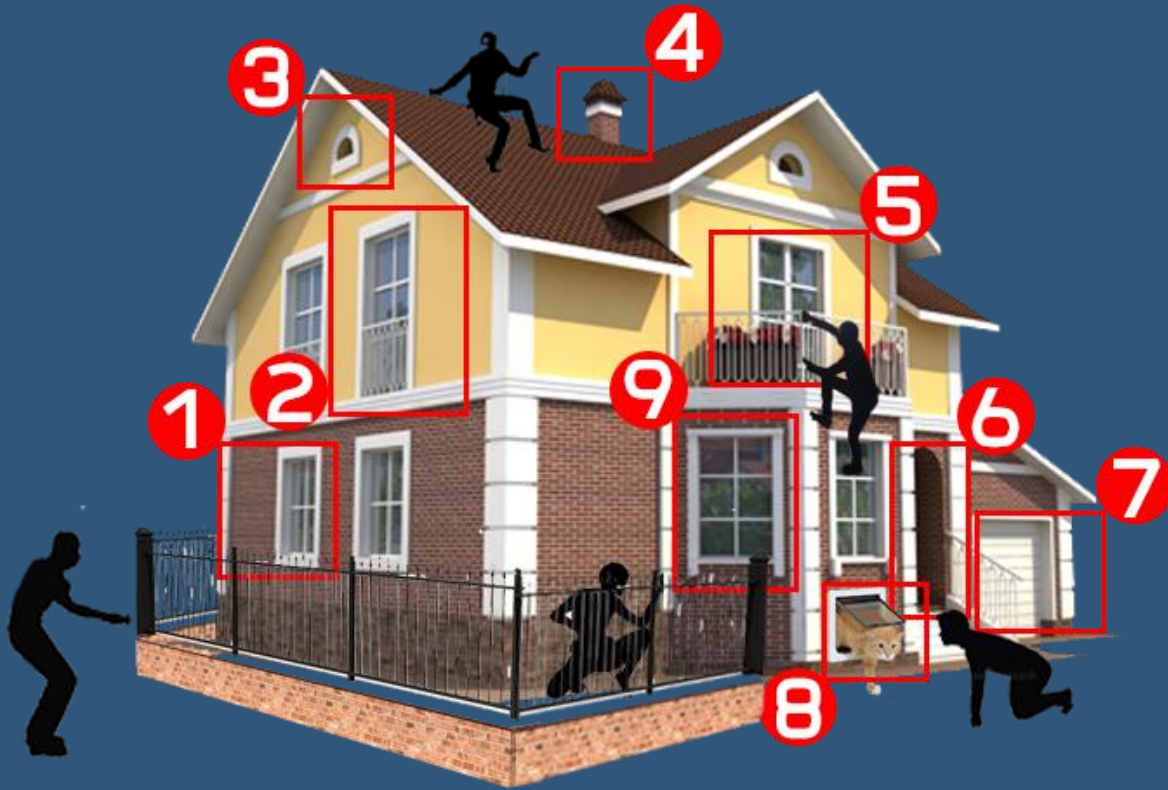
ประเภทของ Ransomware

มัลแวร์เรียกค่าไถ่ หลักรๆ แล้วมี 2 ประเภท คือ: มัลแวร์เรียกค่าไถ่แบบ **Locker** ซึ่งล็อคคอมพิวเตอร์ หรือ อุปกรณ์ และมัลแวร์เรียกค่าไถ่แบบ **Crypto** ซึ่งจะทำการเข้ารหัส เพื่อป้องกันการเข้าถึงไฟล์ หรือข้อมูล โดยมักทำการเข้ารหัสเป็นหลัก



Ransomware

เข้าไปในองค์กรของคุณได้อย่างไร?



<https://www.bitdefender.co.th/post/ransomware/>

Tactic {

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark	Distributed Component	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	Applnit DLLs	Applnit DLLs	Bypass Account					Data Transfer Size Limits	Custom Command and Control

Drive-by Compromise

A drive-by compromise is when an adversary gains access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is targeted for exploitation. This can happen in several ways, but there are a few main components:

Multiple ways of delivering exploit code to a browser exist, including:

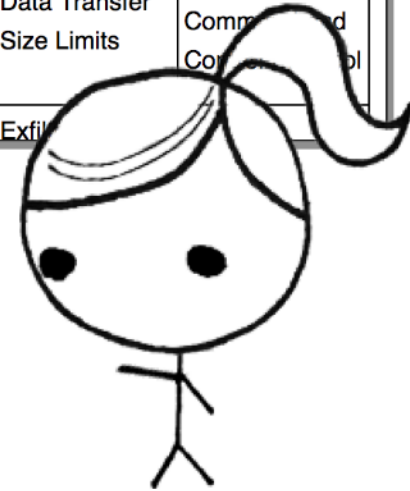
- A legitimate website is compromised where adversaries have injected some form of malicious code such as JavaScript, iFrames, cross-site scripting.
- Malicious ads are paid for and served through legitimate ad providers.
- Built-in web application interfaces are leveraged for the insertion of any other kind of object that can be used to display web content or contain a script that executes on the visiting client (e.g. forum posts, comments, and other user controllable web content).

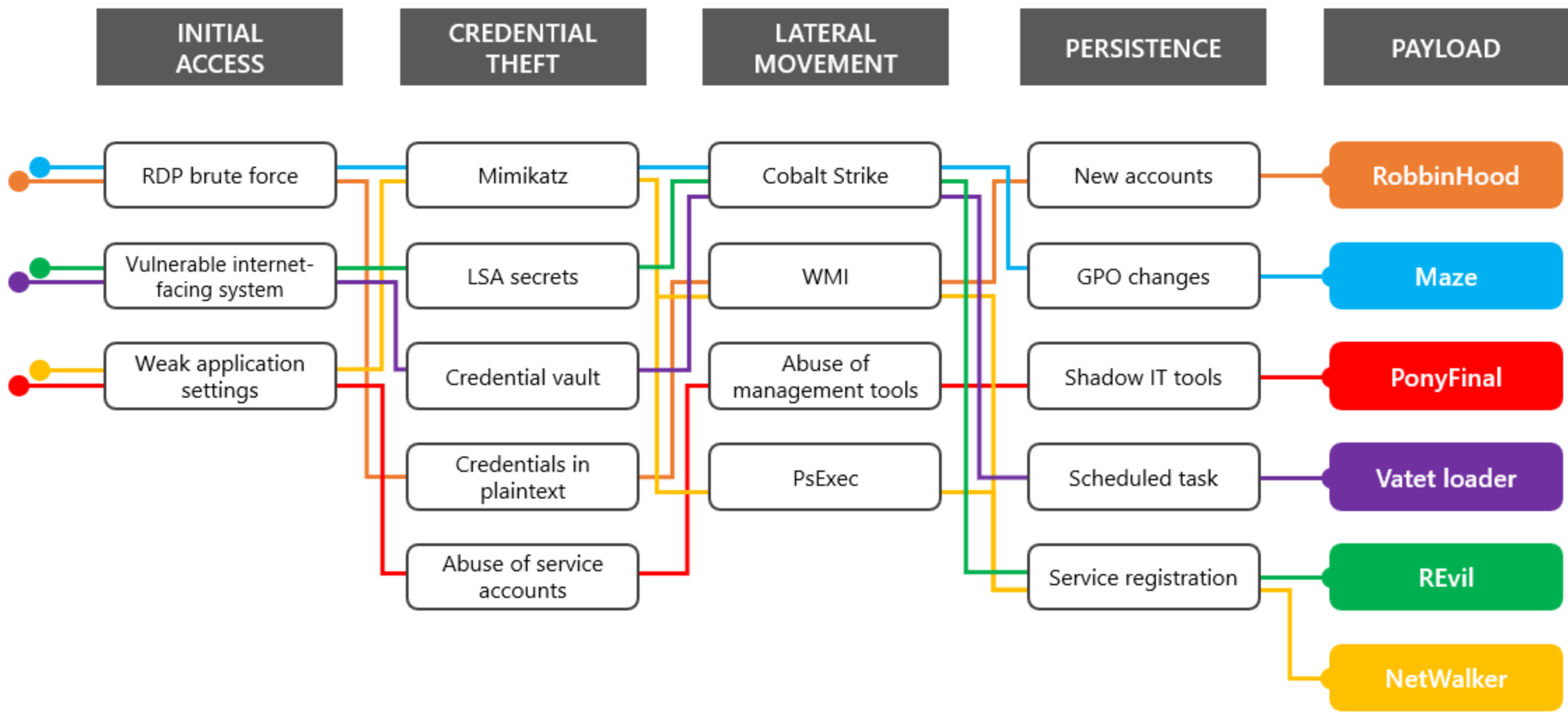
Often the website used by an adversary is one visited by a specific community, such as government, a particular industry, or region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted attack is referred to a strategic web compromise or watering hole attack. There are several known examples of this occurring.^[1]

Drive-by Compromise Technique	
ID	T1189
Tactic	Initial Access
Platform	Linux, Windows, macOS
Permissions Required	User
Data Sources	Packet capture, Network device logs, Process use of network, Web proxy, Network intrusion detection system, SSL/TLS inspection

Technique

Procedure





Concept การกระทำของคนร้าย ในการใช้ Ransomware โจมตี

ขโมยของ



แอบดูลาดเลา



เตรียมอุปกรณ์



เข้าไปค้น



หาสิ่งของมีค่า



เอาออกไป

วันที่ 1

วันที่ 2

วันที่ 3

วันที่...

วันที่เรารู้ตัว

Ransomware



ค้นหาข้อมูลเหยื่อ



หาช่องโหว่



ติดตั้ง



ควบคุมจาก
ทางไกล



ได้ข้อมูลไป







THANK YOU
FOR LISTENING

Section III