Payment system : Risk & Security

Huy Nguyen, PhD

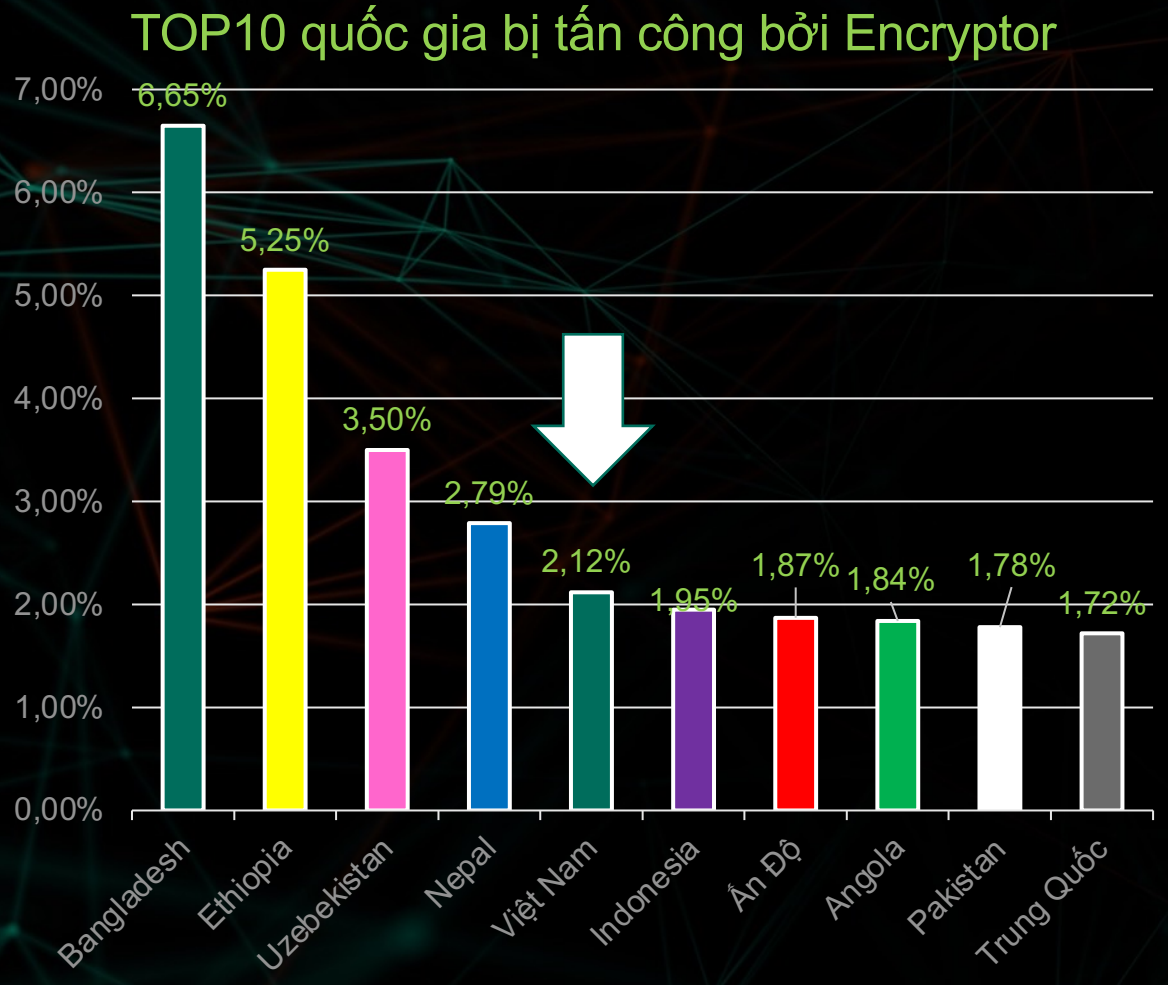
THÔNG KÊ TÌNH HÌNH AN NINH MẠNG NGÀNH TÀI CHÍNH 2019

2019 QUA CÁC CON SỐ

- **30.01%** máy tính người dùng bị nhiễm ít nhất 1 loại mã độc do tấn công từ các Website
- Klab ngăn chặn **1,876,998,691** lượt tấn công từ các nguồn Online
- **554,159,621** các đường dẫn URL được xem là nguy hại
- Web Threat Protection của Klab phát hiện **21,643,946** các đối tượng nguy hại
- **765,538** máy tính là mục tiêu của ransomware
- **5,638,828** máy tính của người bị mã độc đào tiền ảo tấn công
- Klab ngăn ngặn các mã độc có khả năng đánh cắp tiền qua Online Banking trên **830,135** thiết bị

KASPERSKY lab

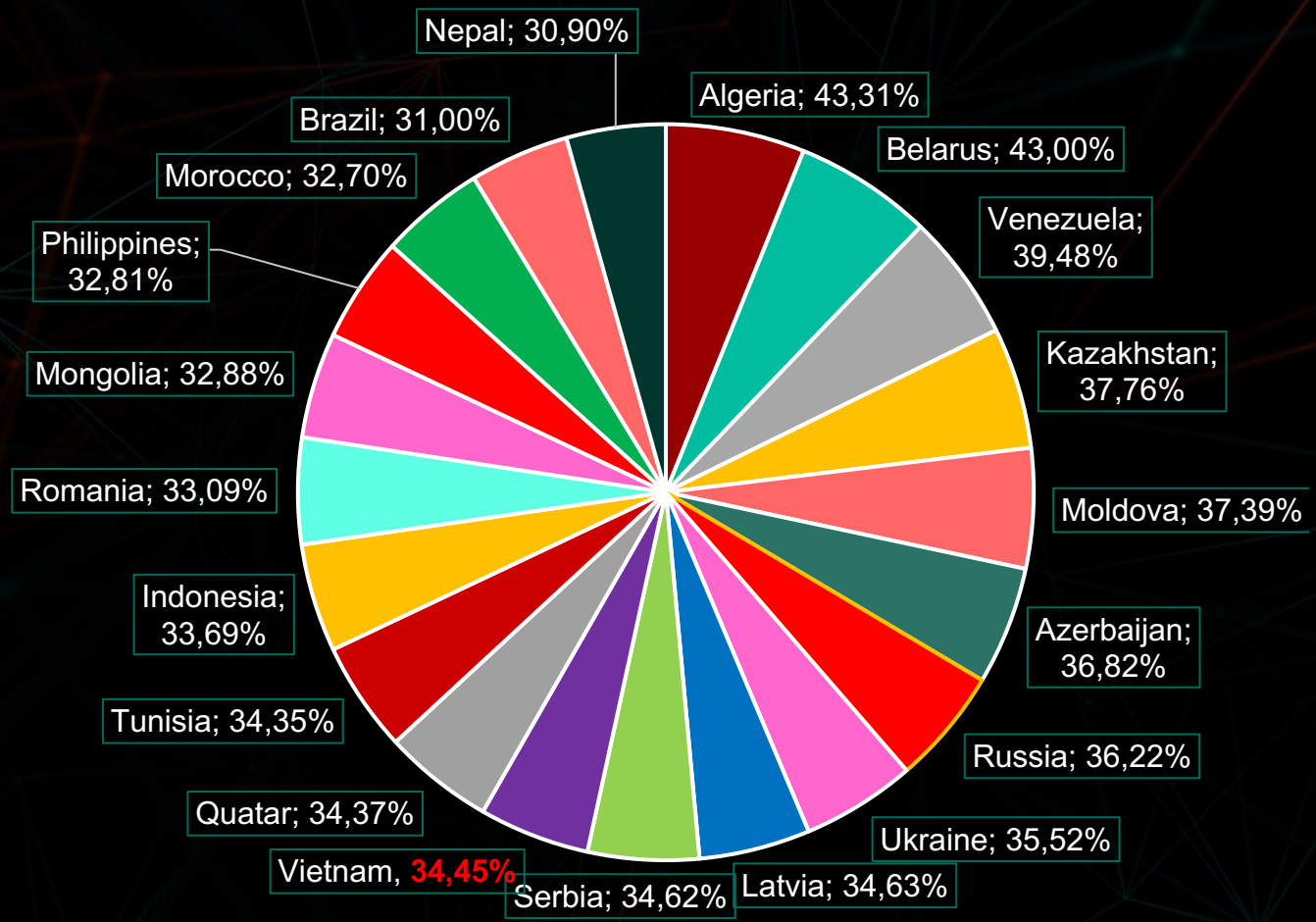
TÌNH HÌNH AN NINH MẠNG TẠI VIỆT NAM 2019



- Loại ransomware nào có tỷ lệ tấn công người dùng cao nhất?
  - ➢ WannaCry – 29%
  - ➢ GandCrab – 6%

KASPERSKY lab

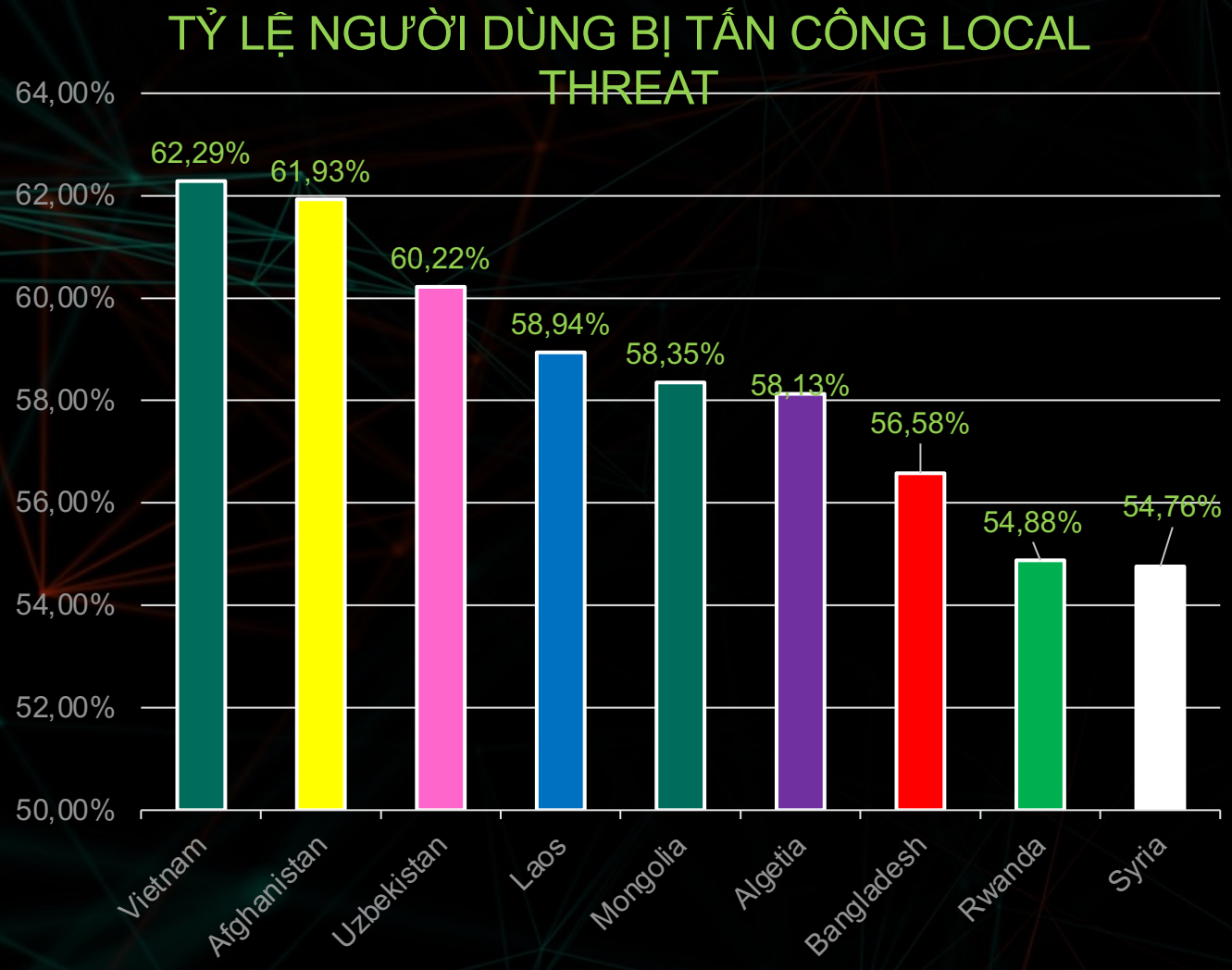
TÌNH HÌNH AN NINH MẠNG TẠI VIỆT NAM 2019



NGƯỜI DÙNG TẠI CÁC QUỐC GIA ĐỐI MẶT VỚI NGUY HIỂM KHI ONLINE

KASPERSKY lab

TÌNH HÌNH AN NINH MẠNG TẠI VIỆT NAM 2019



- Local threat là tấn công phổ biến nhất: lây nhiễm mã độc qua file, USB...

KASPERSKY lab

Báo cáo về cuộc tấn công mạng

OPERATION SHADOWHAMPER

KASPERSKY lab

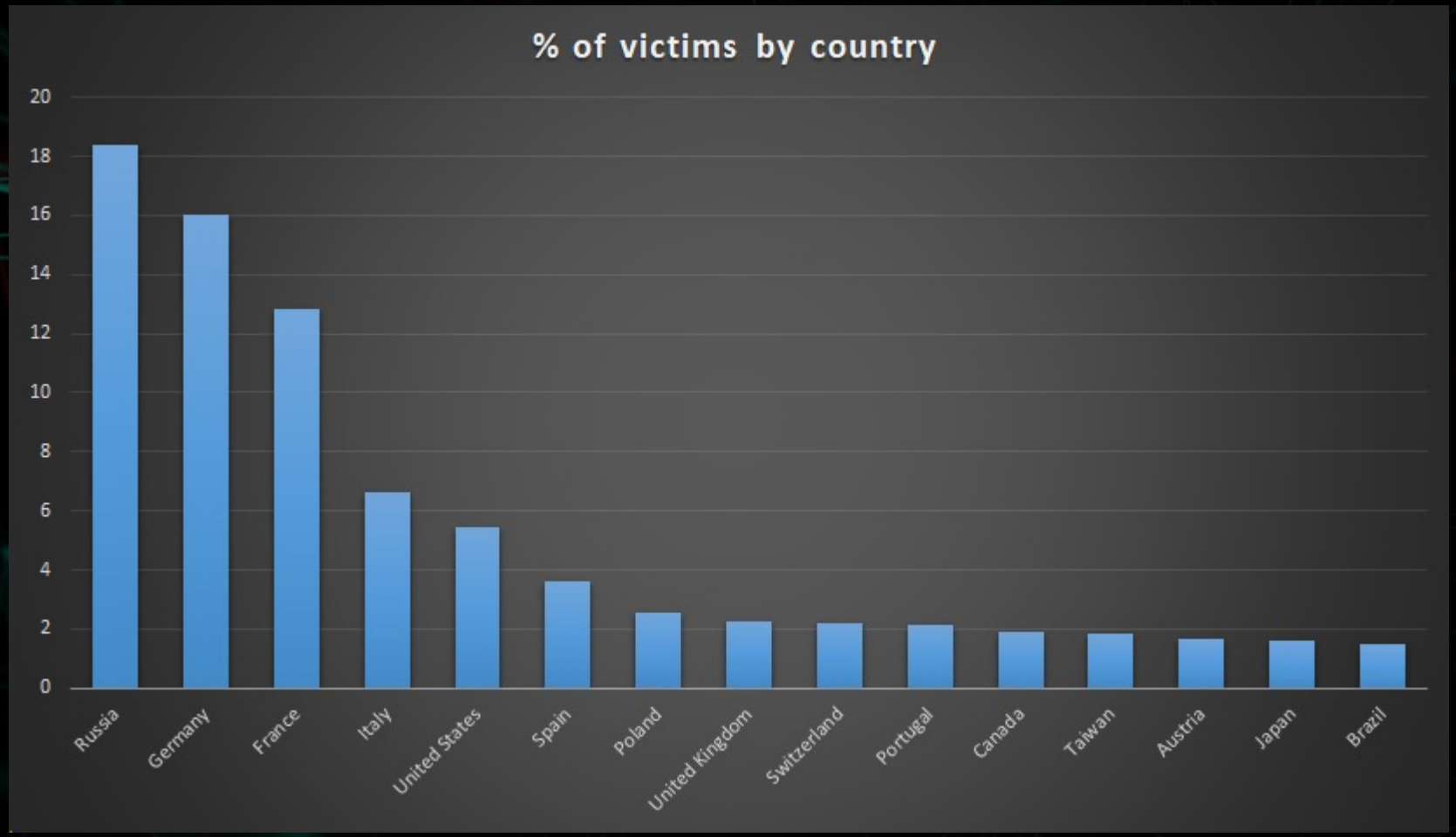
Tấn công có chủ đích Operation ShadowHamper

- ASUS là nhà sản xuất máy tính cá nhân thứ 5 thế giới
- Sử dụng trình tiện ích ASUS Live Update để làm bàn đạp tấn công
- Là một tấn công Supply Chain attack
- Diễn ra từ tháng 6-11/2018
- Khoảng > 1 triệu máy tính bị nhiễm

- 619 địa chỉ MAC được định nghĩa cứng trong source code tấn công:
  - Hacker đã xác định nạn nhân
  - Tấn công và sử dụng ASUS Live Update là 1 phương thức tiếp cận nạn nhân
- Klab đã liên hệ và hỗ trợ ASUS điều tra
- Klab cung cấp trình tiện ích kiểm giúp người sở hữu máy tính ASUS kiểm tra xem địa chỉ MAC của mình có nằm trong danh sách tấn công

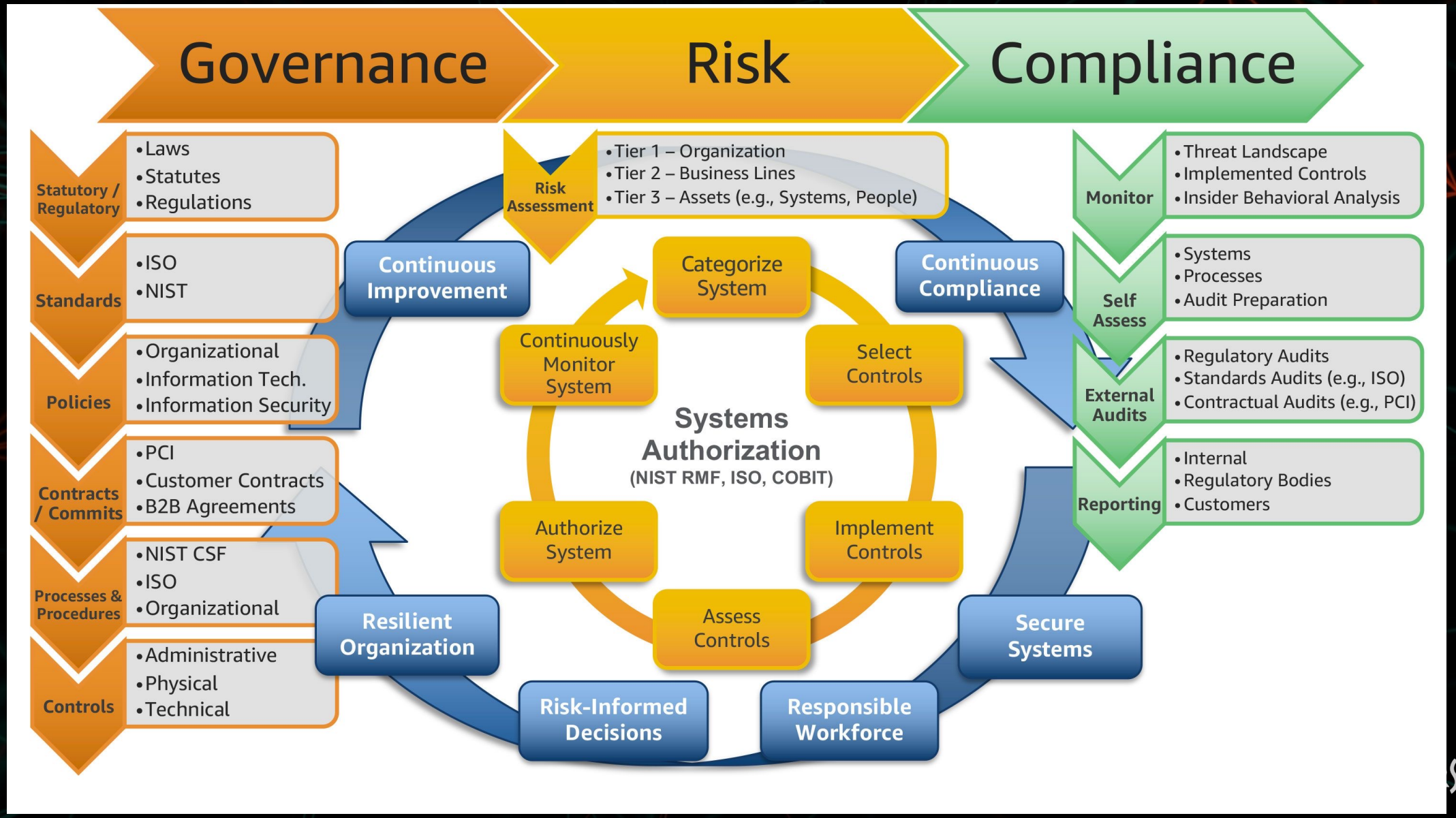
KASPERSKY lab

Tấn công có chủ đích Operation ShadowHamper

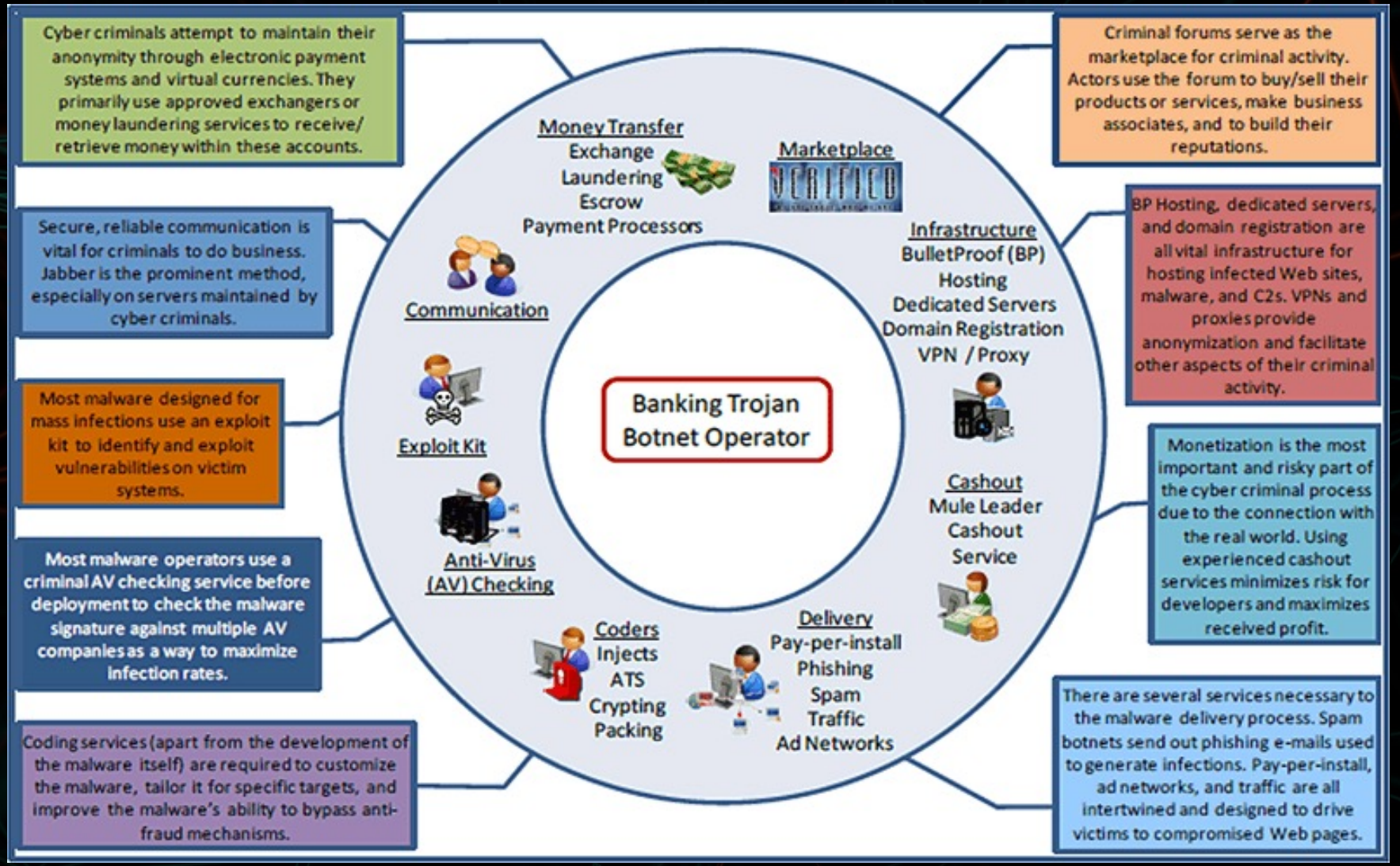


- Bao nhiêu máy tính ASUS tại Việt Nam bị ảnh hưởng?

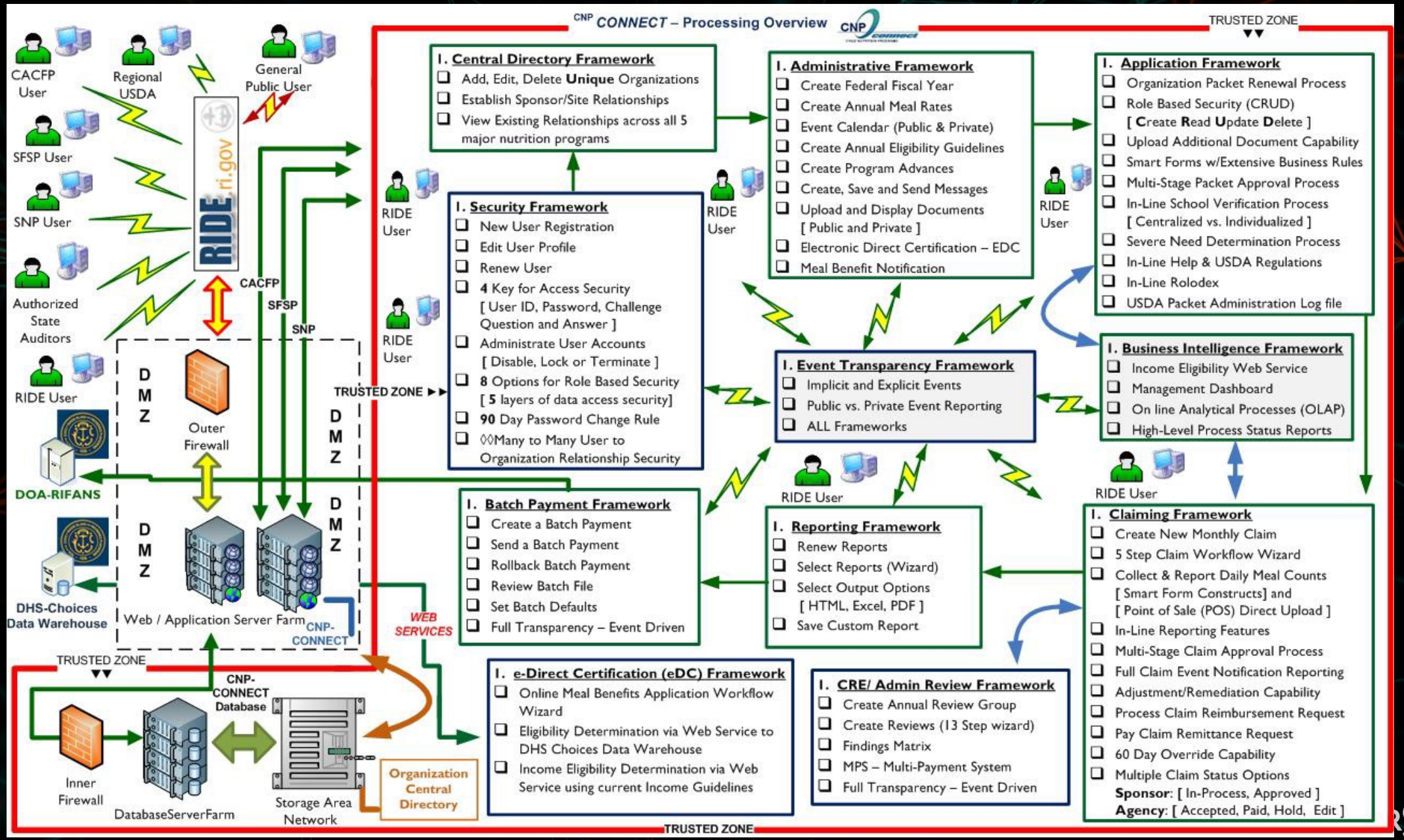
Payment systems : RISK


Governance
Risk
Compliance
Statutory / Regulatory
•Laws
•Statutes
•Regulations
Standards
•ISO
•NIST
Policies
•Organizational
•Information Tech.
•Information Security
Contracts / Commits
•PCI
•Customer Contracts
•B2B Agreements
Processes & Procedures
•NIST CSF
•ISO
•Organizational
Controls
•Administrative
•Physical
•Technical
Risk Assessment
•Tier 1 – Organization
•Tier 2 – Business Lines
•Tier 3 – Assets (e.g., Systems, People)
Continuous Improvement
Continuous Compliance
Resilient Organization
Secure Systems
Risk-Informed Decisions
Responsible Workforce
Categorize System
Select Controls
Implement Controls
Assess Controls
Authorize System
Continuously Monitor System
Systems Authorization
(NIST RMF, ISO, COBIT)
Monitor
•Threat Landscape
•Implemented Controls
•Insider Behavioral Analysis
Self Assess
•Systems
•Processes
•Audit Preparation
External Audits
•Regulatory Audits
•Standards Audits (e.g., ISO)
•Contractual Audits (e.g., PCI)
Reporting
•Internal
•Regulatory Bodies
•Customers

Payment systems : security



KASPERSKY lab


CNP CONNECT – Processing Overview
CNP connect
TRUSTED ZONE
CACFP User
Regional USDA
General Public User
SFSP User
SNP User
Authorized State Auditors
RIDE User
RIDE.ri.gov
CACFP
SFSP
SNP
DMZ
Outer Firewall
DOA-RIFANS
DHS-Choices Data Warehouse
Web / Application Server Farm
CNP-CONNECT
WEB SERVICES
TRUSTED ZONE
CNP-CONNECT Database
Inner Firewall
DatabaseServerFarm
Storage Area Network
Organization Central Directory
1. Central Directory Framework
Add, Edit, Delete Unique Organizations
Establish Sponsor/Site Relationships
View Existing Relationships across all 5 major nutrition programs
1. Security Framework
New User Registration
Edit User Profile
Renew User
4 Key for Access Security [User ID, Password, Challenge Question and Answer]
Administrate User Accounts [Disable, Lock or Terminate]
8 Options for Role Based Security [5 layers of data access security]
90 Day Password Change Rule
◊◊Many to Many User to Organization Relationship Security
1. Administrative Framework
Create Federal Fiscal Year
Create Annual Meal Rates
Event Calendar (Public & Private)
Create Annual Eligibility Guidelines
Create Program Advances
Create, Save and Send Messages
Upload and Display Documents [Public and Private]
Electronic Direct Certification – EDC
Meal Benefit Notification
1. Application Framework
Organization Packet Renewal Process
Role Based Security (CRUD) [Create Read Update Delete]
Upload Additional Document Capability
Smart Forms w/Extensive Business Rules
Multi-Stage Packet Approval Process
In-Line School Verification Process [Centralized vs. Individualized]
Severe Need Determination Process
In-Line Help & USDA Regulations
In-Line Rolodex
USDA Packet Administration Log file
1. Event Transparency Framework
Implicit and Explicit Events
Public vs. Private Event Reporting
ALL Frameworks
1. Business Intelligence Framework
Income Eligibility Web Service
Management Dashboard
On line Analytical Processes (OLAP)
High-Level Process Status Reports
1. Batch Payment Framework
Create a Batch Payment
Send a Batch Payment
Rollback Batch Payment
Review Batch File
Set Batch Defaults
Full Transparency – Event Driven
1. Reporting Framework
Renew Reports
Select Reports (Wizard)
Select Output Options [HTML, Excel, PDF]
Save Custom Report
1. Claiming Framework
Create New Monthly Claim
5 Step Claim Workflow Wizard
Collect & Report Daily Meal Counts [Smart Form Constructs] and [Point of Sale (POS) Direct Upload]
In-Line Reporting Features
Multi-Stage Claim Approval Process
Full Claim Event Notification Reporting
Adjustment/Remediation Capability
Process Claim Reimbursement Request
Pay Claim Remittance Request
60 Day Override Capability
Multiple Claim Status Options
Sponsor: [In-Process, Approved]
Agency: [Accepted, Paid, Hold, Edit]
1. e-Direct Certification (eDC) Framework
Online Meal Benefits Application Workflow Wizard
Eligibility Determination via Web Service to DHS Choices Data Warehouse
Income Eligibility Determination via Web Service using current Income Guidelines
1. CRE/ Admin Review Framework
Create Annual Review Group
Create Reviews (13 Step wizard)
Findings Matrix
MPS – Multi-Payment System
Full Transparency – Event Driven
RIDE User
TRUSTED ZONE

How the Carbanak cybergang stole $1bn

A targeted attack on a bank

1. Infection

Carbanak backdoor sent as an attachment

Bank employee

Emails with exploits

Credentials stolen

100s of machines infected
in search of the admin PC

2. Harvesting Intelligence

Intercepting the clerks' screens

3. Mimicking the staff

How the money was stolen

Online-banking
Money was transferred to fraudsters' accounts

E-payment systems
Money was transferred to banks in China and the US

Inflating account balances
The extra funds were pocketed via a fraudulent transaction

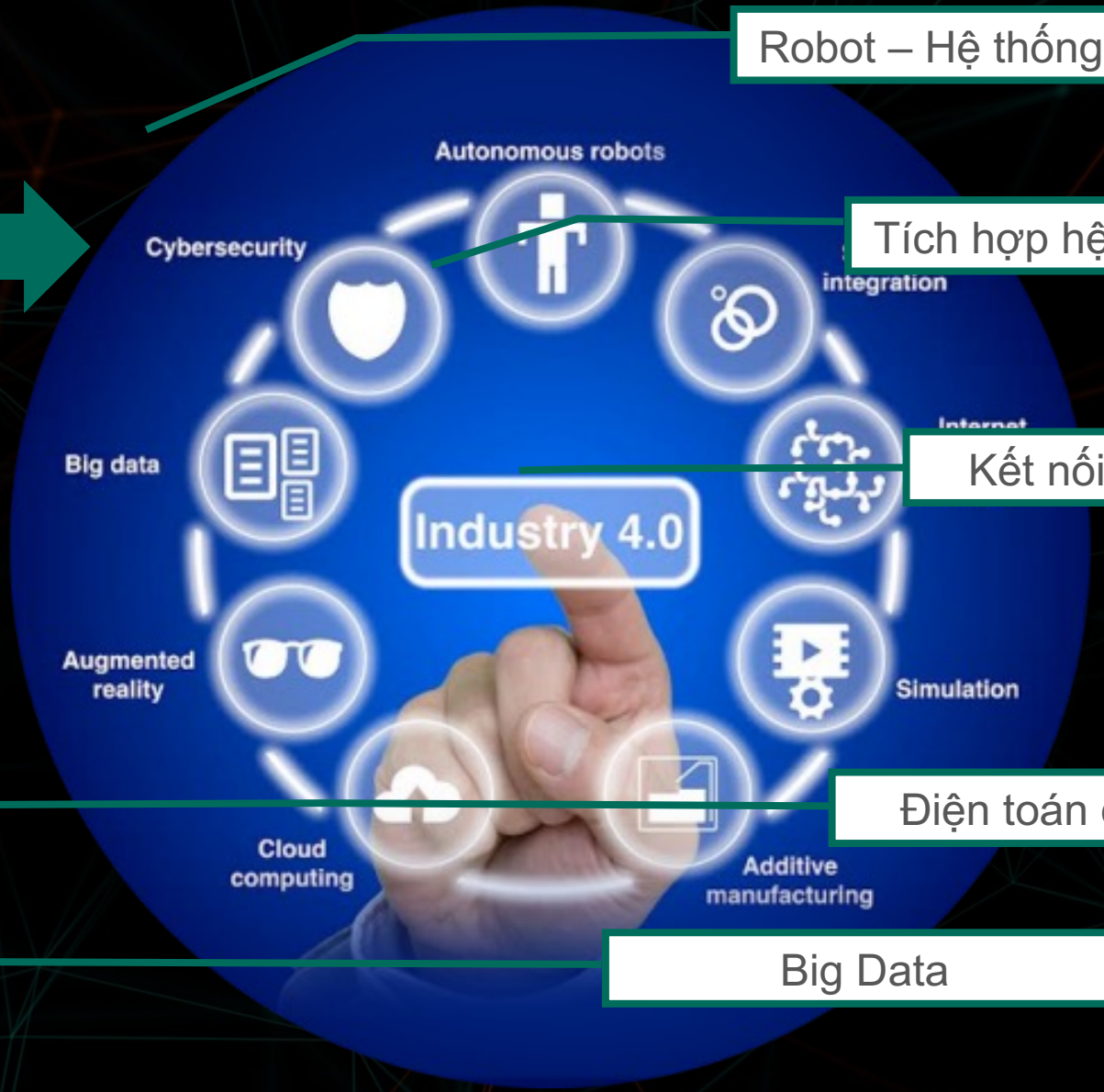
Controlling ATMs
Orders to dispense cash at a pre-determined time

GREAT KASPERSKY lab

AN NINH MẠNG TRONG CMCN 4.0

CÔNG NGHIỆP 4.0 – THỬ THÁCH AN NINH MẠNG MỚI

SẢN XUẤT



Robot – Hệ thống sản xuất

Tích hợp hệ thống đối tác

Kết nối vạn vật - IoT

Điện toán đám mây

Big Data

CNTT

KASPERSKY lab

BẢO MẬT TỔNG THỂ, BAO GỒM HẠ TẦNG CÔNG NGHIỆP — Nhận thức thấp

CEO

Chưa nhìn thấy An ninh mạng mang lại giá trị về Doanh thu, Quản lý rủi ro trong hệ thống sản xuất

Đội ngũ bảo mật

Không được phép vào khu vực sản xuất công nghiệp

Kỹ sư sản xuất

Quan tâm nhiều đến An toàn lao động hơn là An toàn thông tin

Nhân viên

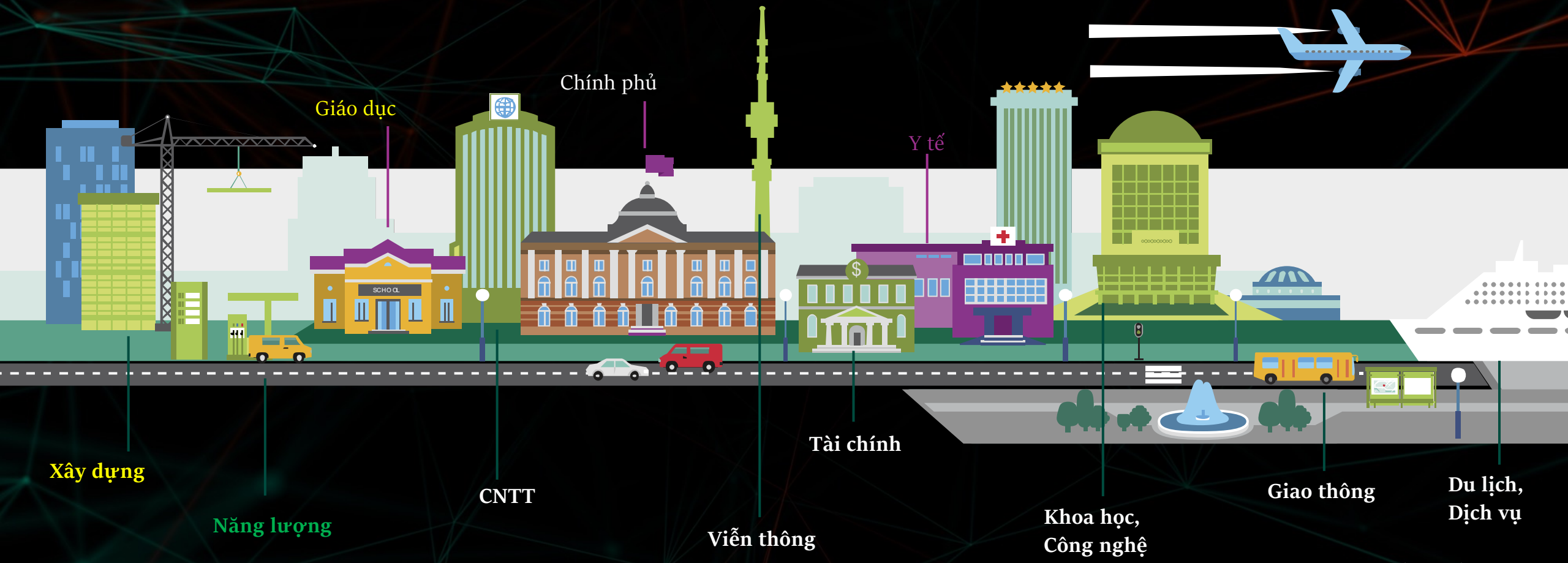
Phó thác bảo mật cho đội ngũ quản trị viên

Hiểu biết lẫn nhau, 4 bên hợp tác là rất quan trọng để đảm bảo An ninh mạng thành công và Bảo vệ vững chắc hệ thống cơ sở hạ tầng quan trọng.

KASPERSKY lab

THẾ GIỚI KẾT NỐI

MỞ RỘNG KẾT NỐI ĐỒNG NGHĨA NHIỀU RỦI RO



SỰ PHÁT TRIỂN CỦA CÁC MỐI ĐE DỌA

1994

1
VIRUS MỚI
MỖI GIỜ

2006

13
VIRUS MỚI
MỖI PHÚT

2011

1XXX
VIRUS MỚI
MỖI GIÂY

2017

323,000
MÃ ĐỘC MỚI
MỐI NGÀY

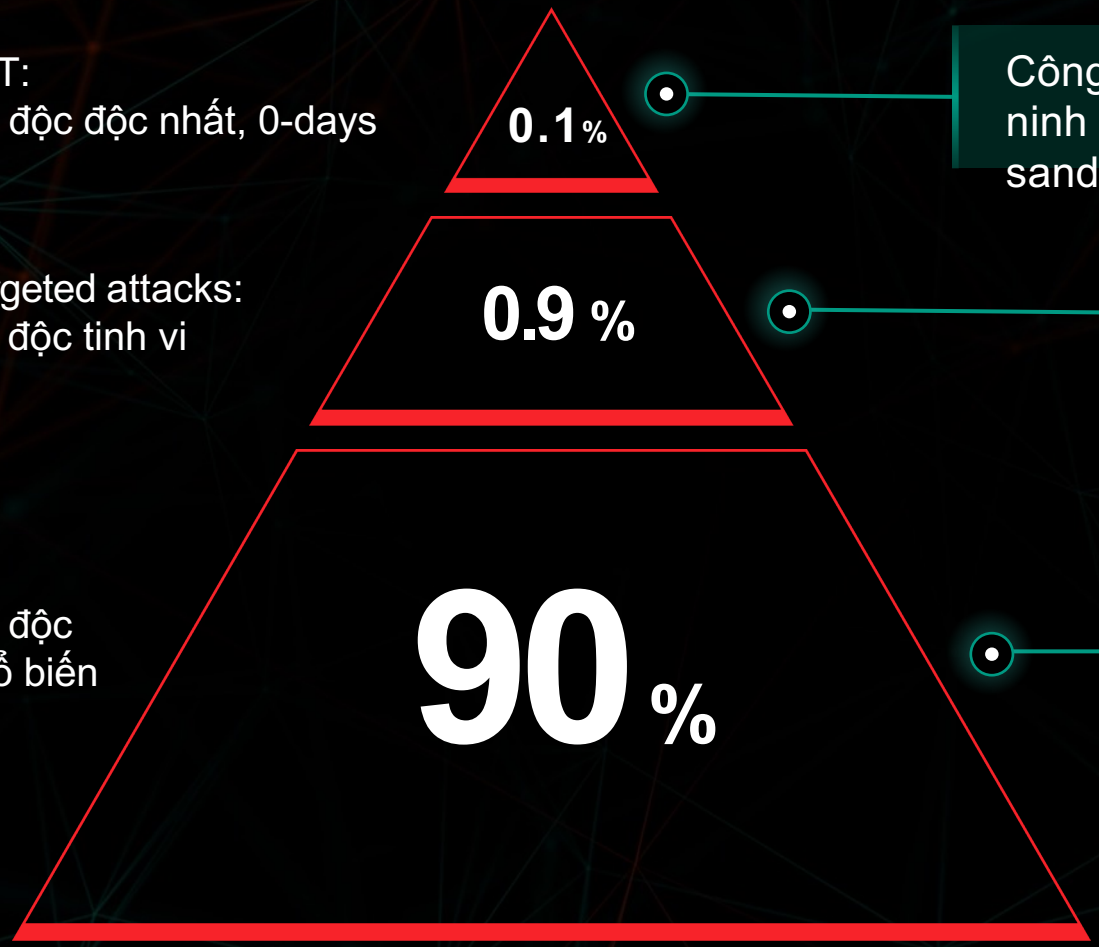
KASPERSKY lab

MỐI ĐE DỌA CÓ TỶ LỆ NHỎ GÂY RA NHỮNG RỦI RO LỚN

APT:
Mã độc độc nhất, 0-days

Targeted attacks:
Mã độc tinh vi

Mã độc
Phổ biến



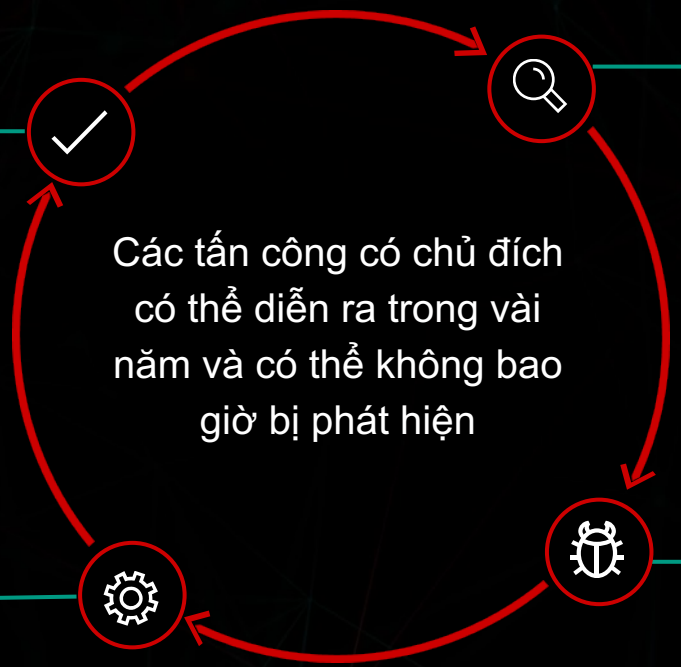
Công nghệ học máy, Mối đe dọa an ninh mạng toàn cầu, công nghệ sandboxing tiên tiến

Phân tích hành vi, Heuristic
Điện toán đám mây

Dựa trên Signature
và luật lệ

KASPERSKY lab

TẤN CÔNG MẠNG LÀ KHÔNG NGỪNG:
TẤN CÔNG VẪN LUÔN TRONG TIẾN TRÌNH



CHUẨN BỊ

— Nghiên cứu mục tiêu
— Xây dựng chiến lược
— Chuẩn bị công cụ

LÂY NHIỄM

— Đánh giá điểm yếu
— Vượt qua phòng thủ mạng biên

MỞ RỘNG TRUY CẬP

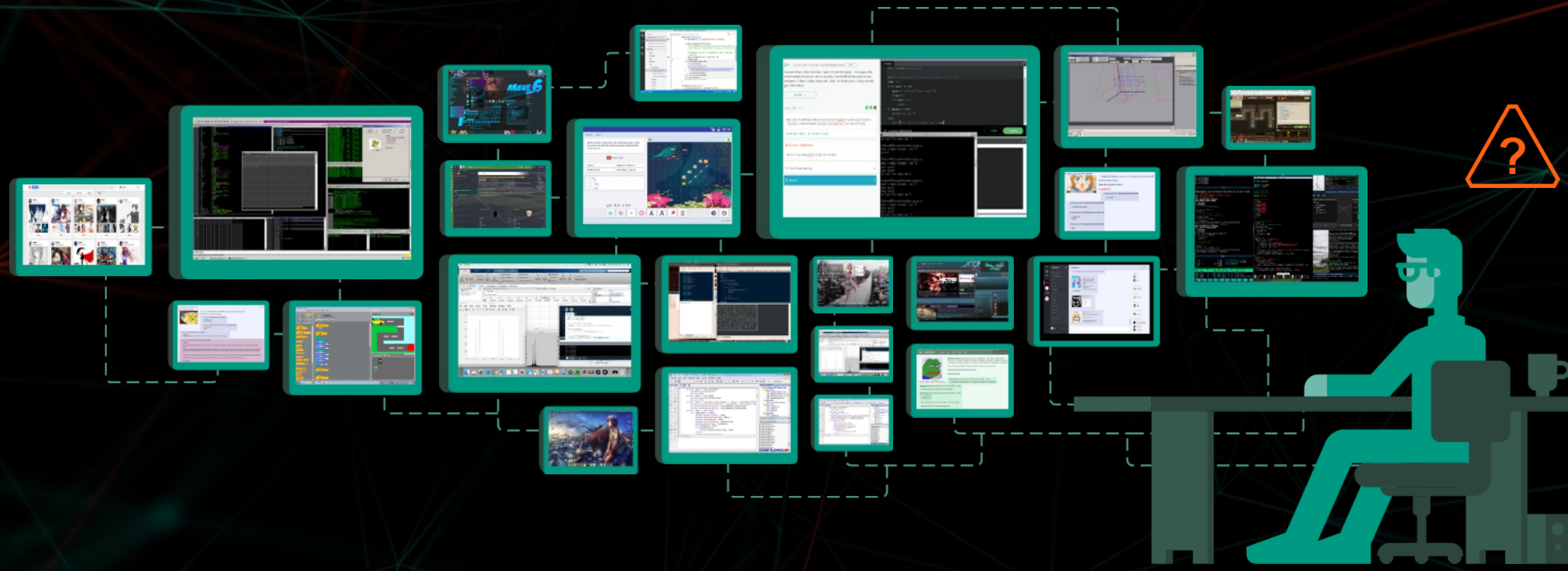
— Đánh cắp
— Nâng cấp đặc quyền
— Tấn công mở rộng
— Kiểm soát mục tiêu

KHAI THÁC

— Hoạt động ẩn giấu
— Giải nén dữ liệu
— Xử lý dấu vết
— Rút lui lặng lẽ

KASPERSKY lab

…NHIỀU GIẢI PHÁP BẢO VỆ, VÀ MỖI GIẢI PHÁP CÓ 1 GIAO DIỆN QUẢN TRỊ RIÊNG BIỆT



KASPERSKY lab

BÂY GIỜ LÀ THỜI ĐIỂM XÂY DỰNG MỘT TRUNG TÂM AN NINH MẠNG - SOC

DISCOVER

BÂY GIỜ LÀ THỜI ĐIỂM XÂY DỰNG MỘT TRUNG TÂM AN NINH MẠNG - SOC

DISCOVER

KASPERSKY lab

Bài tập 2:

- Cung cấp vài công cụ dò quét lỗ hổng của hệ thống, đặt biệt là hệ thống than toán và hệ thống thanh toán trên thương mại điện tử.

- Giả lập tấn công hệ thống thanh toán, các phương thức phòng thủ và đánh trả