ELECS425F
Computer and Network Security

Lec 01

Outline

- Introduction
- Security Basic

The computer security problem

- Lots of buggy software
- Social engineering is very effective
- Money can be made from finding and exploiting vulnerabilities

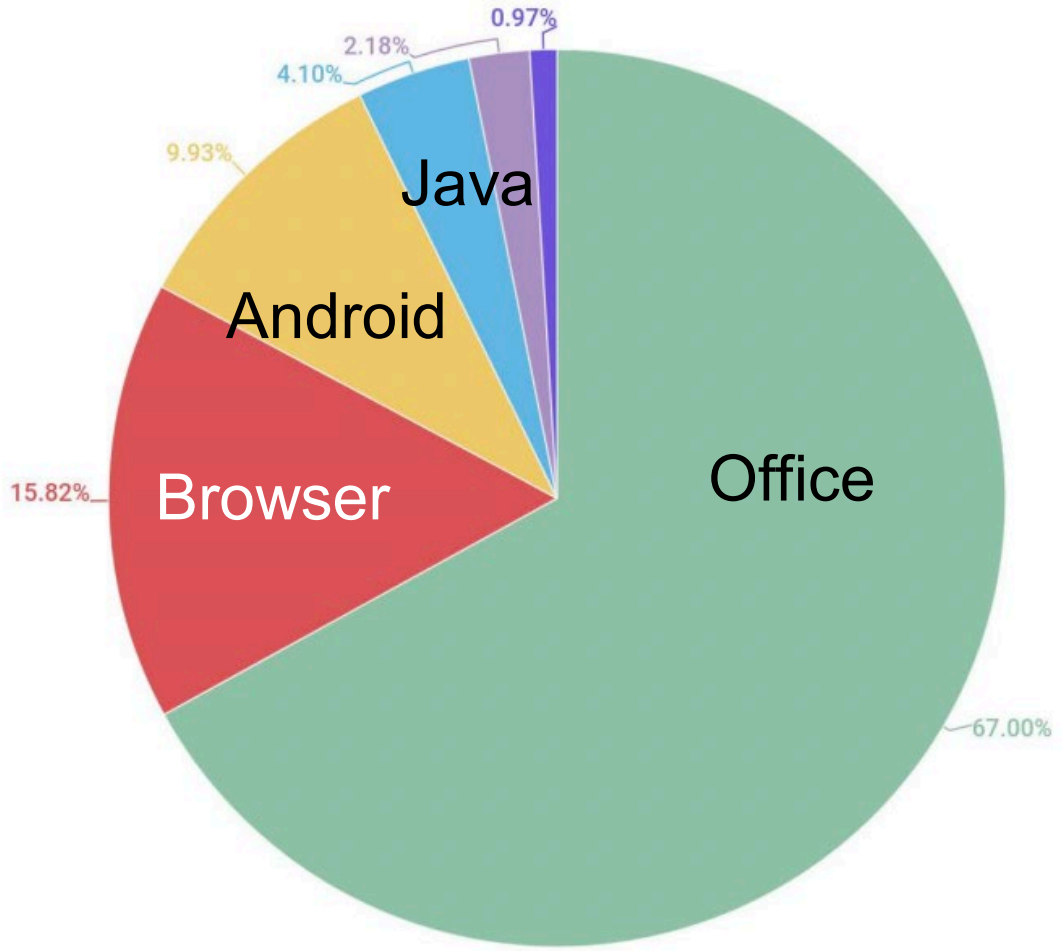
Top 10 products by total number of “distinct” vulnerabilities in 2019

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Android	Google	OS	414
2	Debian Linux	Debian	OS	360
3	Windows Server 2016	Microsoft	OS	357
4	Windows 10	Microsoft	OS	357
5	Windows Server 2019	Microsoft	OS	351
6	Acrobat Reader Dc	Adobe	Application	342
7	Acrobat Dc	Adobe	Application	342
8	Cpanel	Cpanel	Application	321
9	Windows 7	Microsoft	OS	250
10	Windows Server 2008	Microsoft	OS	248

Top 10 products by total number of “distinct” vulnerabilities in 2021

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Debian Linux	Debian	OS	5685
2	Android	Google	OS	4042
3	Ubuntu Linux	Canonical	OS	3091
4	Mac Os X	Apple	OS	2958
5	Linux Kernel	Linux	OS	2733
6	Fedora	Fedoraproject	OS	2656
7	Iphone Os	Apple	OS	2570
8	Windows 10	Microsoft	OS	2569
9	Windows Server 2016	Microsoft	OS	2318
10	Chrome	Google	Application	2299
11	Windows Server 2008	Microsoft	OS	2144

Vulnerable applications being exploited



Source: Kaspersky Security Bulletin 2020

What motivates attackers?

- Why compromise end user machines?
- Why own machines?
- Why compromise end user machines?
- …….

Why compromise end user machines?

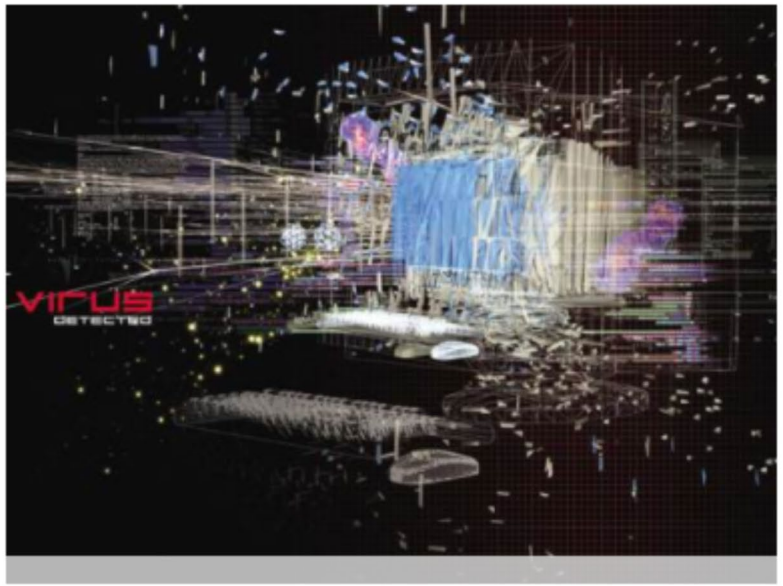
Experts sound alarm on Silentbanker Trojan

By Shaun Nichols
Jan 16 2008
7:07AM

0 Comments

Researchers have uncovered a new banking Trojan which steals user data from more than 400 banks worldwide..

Trojan.Silentbanker intercepts account information, redirects traffic to phishing sites, and even alters transactions to send money to the attacker's bank account.

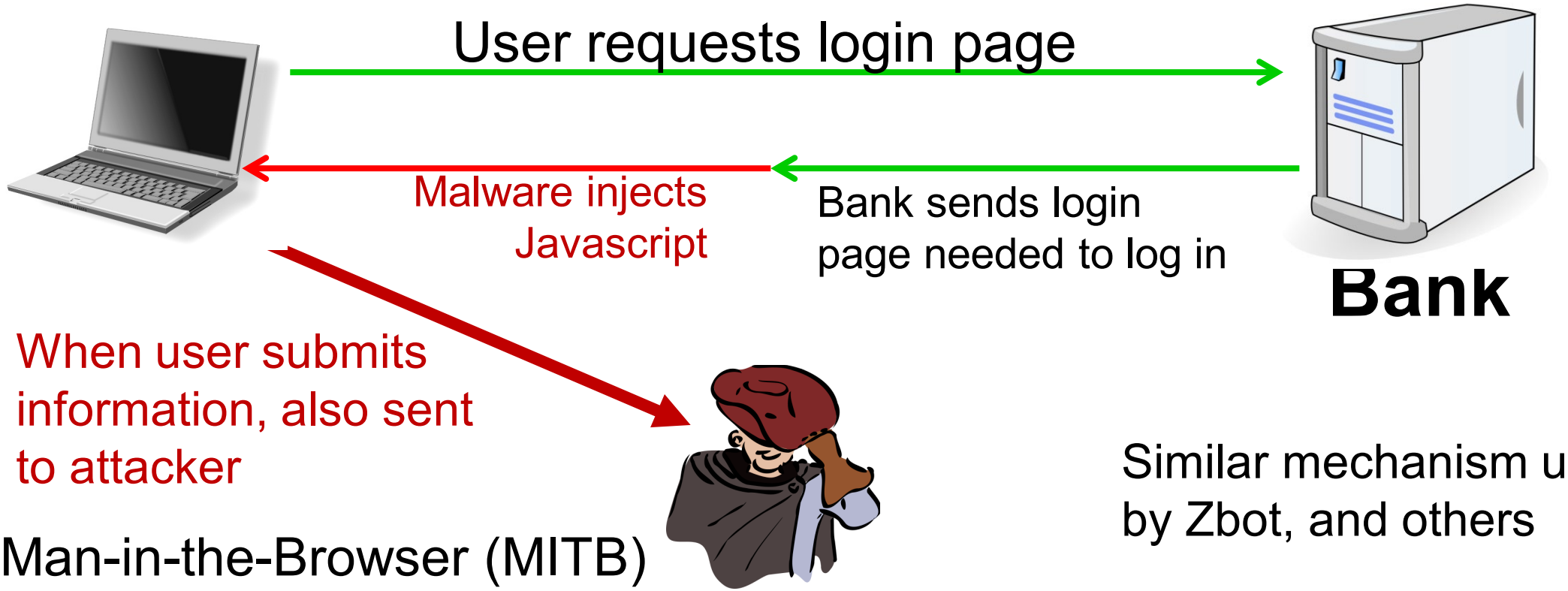


Why compromise end user machines?

1. Steal user credentials

keylog for banking passwords, corporate passwords, gaming pwds

Example: **SilentBanker** (and many like it)



Similar mechanism used by Zbot, and others

Why own machines?

Hong Kong / Hong Kong economy

Global ransomware attack hits third Hong Kong system

Experts warn Hongkongers to take preventative measures as 'WannaCry' cyberattack affects more than 100,000 computers worldwide

Why own machines?

2. Ransomware

	Name	% of attacked users**
1	WannaCry	7.71
2	Locky	
3	Cerber	5.89
4	Jaff	2.58
5	Cryrar/ACCDFISA	2.20
6	Spora	2.19
7	Purgen/GlobeImposter	2.11
8	Shade	2.06
9	Crysis	1.25
10	CryptoWall	1.13

- Worm spreads via a vuln. in SMB (port 445)
- Apr. 14, 2017: Eternalblue vuln. released by ShadowBrokers
- May 12, 2017: Worm detected (3 weeks to weaponize)

Why compromise end user machines?

The economics of Spam: 0.00000008% response rate = $3.5M turnover

Published Nov. 12, 2008

By Joel Cere

Academics at Berkeley used the "Storm botnet" network to blast 350 million emails for "male enhancement products" at a cost of about $80 per million emails sent. 28 sales resulted with an average purchase price of $100. They estimated that such campaigns when fully utilising the network could mean gross revenues of $7,000 to $9,500 a day, or $3.5 million a year for the spammers.

Why compromise end user machines?
3. IP address and bandwidth stealing

Attacker's goal: look like a random Internet user

Use the IP address of infected machine or phone for:

- **Spam** (e.g. the storm botnet)

  Spamalytics: 1:12M pharma spams leads to purchase

  1:260K greeting card spams leads to infection

- **Denial of Service:** Services: 1 hour (20$), 24 hours (100$)
- **Click fraud** (e.g. Clickbot.a)

The Marketplace for Vulnerabilities

Google Bug Hunters

Reward amounts for security vulnerabilities

New! Vulnerabilities in the Google Cloud Platform are also eligible for additional rewards under the GCP VRP Prize. The total prize money is $313,337 including a top prize of $133,337. See our announcement and the official rules for details and nominate your vulnerability write-ups for the prize here.

Rewards for qualifying bugs range from $100 to $31,337. The following table outlines the usual rewards chosen for the most common classes of bugs. To read more about our approach to vulnerability rewards you can read our article here

Category	Examples	Applications that permit taking over a Google account [1]	Other highly sensitive applications [2]	Normal Google applications	Non-integrated acquisitions and other sandboxed or lower priority applications [3]
Vulnerabilities giving direct access to Google servers					
Remote code execution	"Command injection, deserialization bugs, sandbox escapes"	$31,337	$31,337	$31,337	$1,337 - $5,000
Unrestricted file system or	"Unsandboxed XXE, SQL	$13,337	$13,337	$13,337	$1,337 -

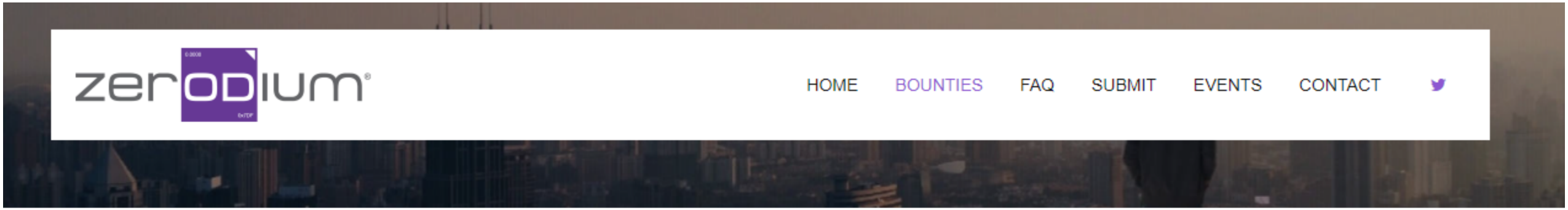
Program Name	Start date	Last Updated	End date	Eligible entries	Bounty Range
Microsoft Azure	2014-09-23	2021-10-18	Ongoing	Vulnerability reports on Microsoft Azure cloud services	Up to $60,000 USD
Microsoft Identity	2018-07-17	2019-10-23	Ongoing	Vulnerability reports on Identity services, including Microsoft Account, Azure Active Directory, or select OpenID standards.	Up to $100,000 USD
Xbox	2020-01-30	2020-01-30	Ongoing	Vulnerability reports on the Xbox Live network and services	Up to $20,000 USD
Microsoft Online Services	2014-09-23	2019-08-05	Ongoing	Vulnerability reports on applicable Microsoft cloud services, including Office 365	Up to $20,000 USD
Microsoft Azure DevOps Services	2019-01-17	2019-01-17	Ongoing	Vulnerability reports on applicable Microsoft Azure DevOps Services	Up to $20,000 USD
Microsoft Dynamics 365 and Power Platform	2019-07-17	2021-10-13	Ongoing	Vulnerablility reports on applicable Microsoft Dynamics 365 and Power Platform applications	Up to $20,000 USD
Microsoft .NET	2016-09-01	2020-11-20	Ongoing	Vulnerability reports on .NET Core and ASP.NET Core RTM and future builds (see link for program details)	Up to $15,000 USD

The Marketplace for Vulnerabilities

Option 1: bug bounty programs (many)

- Google Vulnerability Reward Program: up to $31,337
- Microsoft Bounty Program: up to $100K
- Apple Bug Bounty program: up to $200K
- Stanford bug bounty program: up to $1K
- Pwn2Own competition: $15K

The Marketplace for Vulnerabilities



Zerodium Exploit Acquisition Program

Program Overview

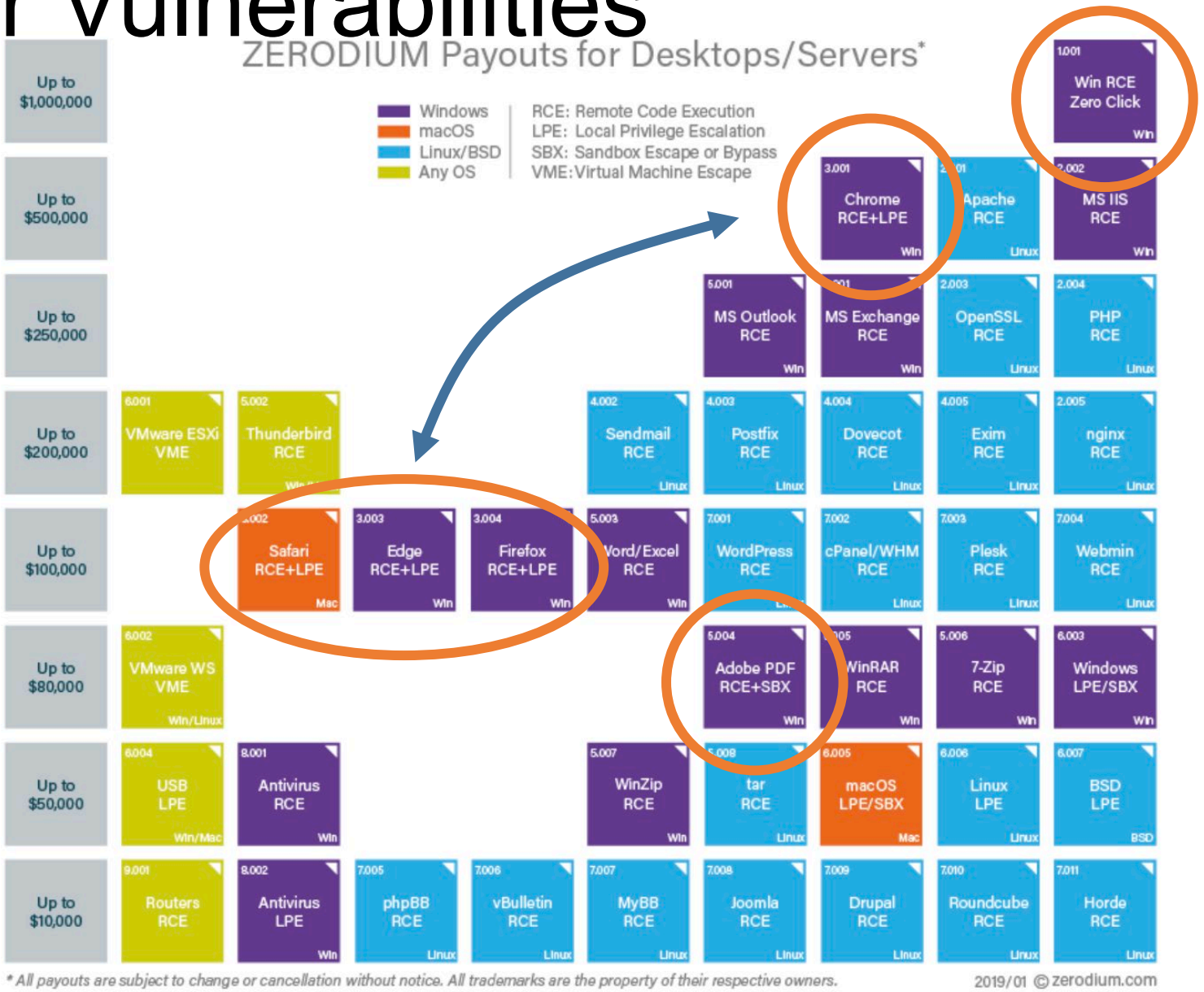
Zerodium pays **BIG bounties** to security researchers to acquire their original and previously unreported zero-day research. While the majority of existing bug bounty programs accept almost any type of vulnerabilities and PoCs but pay very little, **at Zerodium we focus on high-risk vulnerabilities with fully functional exploits** and we pay the highest rewards in the market (**up to $2,500,000 per submission**).

Marketplace for Vulnerabilities

RCE: remote code execution

LPE: local privilege escalation

SBX: sandbox escape



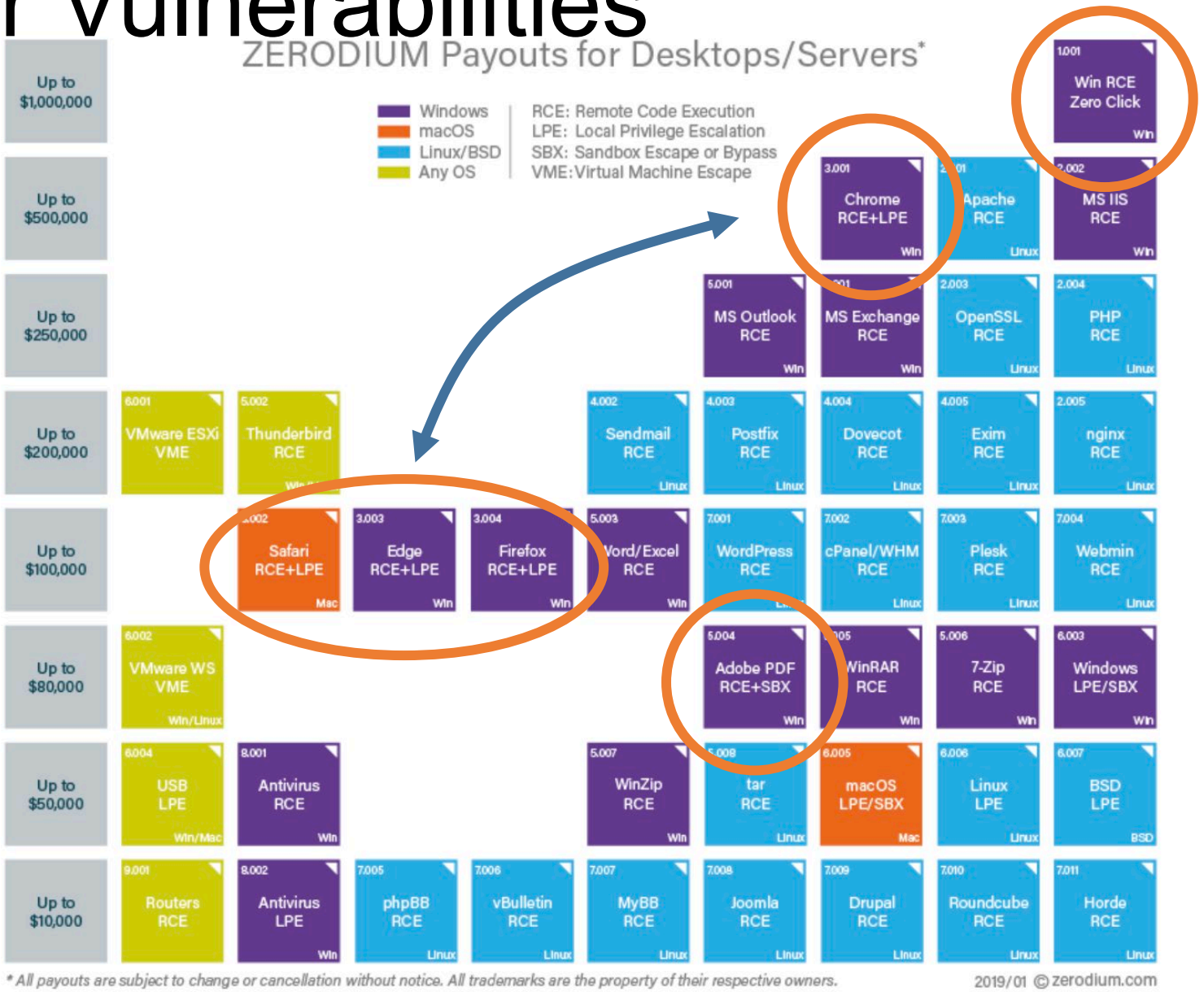
Source: Zerodium payouts

Marketplace for Vulnerabilities

RCE: remote code execution

LPE: local privilege escalation

SBX: sandbox escape



Source: Zerodium payouts

The Marketplace for Vulnerabilities

Option 2:

- Zerodium: up to $2M for iOS, $2.5M for Android (since 2019)
- Zerodayinitiave:

趨勢科技 ZDI 漏洞懸賞計劃 穩居全球最大漏洞揭露機構地位

獨立研究機構 Omdia 指出 2020 年 ZDI 通報全球 60.5% 漏洞

【2021年5月27 日香港訊】全球網絡保安方案領導廠商**趨勢科技**（東京證券交易所股票代碼：**4704**）今天表示，根據獨立研究機構 Omdia 最新調查，趨勢科技的 Zero Day Initiative（ZDI）漏洞懸賞計劃在 2020 年揭露了全球 60.5% 的漏洞，連續 13 年保持全球最大與廠商無關的獨立漏洞懸賞計劃的地位。ZDI 在所有嚴重等級的漏洞中皆擁有最多通報數量，而重大或高嚴重性漏洞的通報量更佔總數的 77%。

The Marketplace for Vulnerabilities

- Why buy 0days?

How the acquired security research is used by ZERODIUM?

ZERODIUM extensively tests, analyzes, validates, and documents all acquired vulnerability research and reports it, along with protective measures and security recommendations, solely to its clients subscribing to the ZERODIUM Zero-Day Research Feed.

Who are ZERODIUM's customers?

ZERODIUM customers are government organizations (mostly from Europe and North America) in need of advanced zero-day exploits and cybersecurity capabilities.

Outline

- Introduction
- Security Basics

What do we mean by security?

Security is about protecting *assets* against possible *threats*.

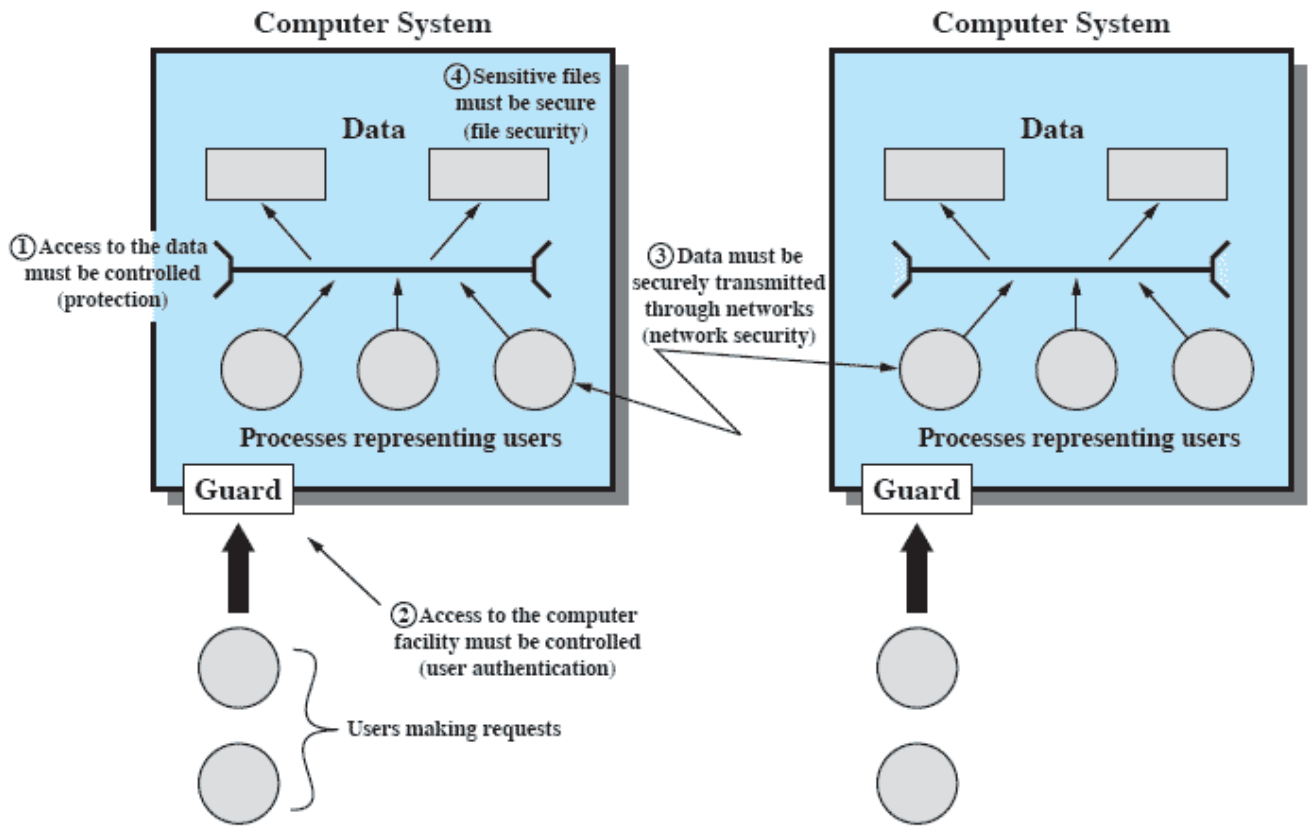
- In particular we are concerned with computer security, but primarily in the sense of *information security*.

Assets are anything we possess of value or use to us.

- A computer system consists of **hardware**, **software** and **data**, each of which is an asset.

A **threat** is something which potentially violates security. It exists when there is a circumstance, capability, action or event that could breach security and cause harm. In other words, a threat is a possible danger that might exploit a vulnerability.

Scope of Computer Security



Goals of security

Confidentiality

- Information about system or its users cannot be learned by an attacker

Integrity

- The system continues to operate properly, only reaching states that would occur if there were no attacker

Availability

- Actions by an attacker do not prevent users from having access to use of the system.

- There is a cost in achieving those goals, and one needs to balance this cost against what you can gain.

Goals of security

The other three concepts of security

Authentication (Verifying who you are)

- Authentication is the process of verifying who you are. When you log on to a PC with a user name and password you are authenticating.

Authorization (checking if you are permitted to access the resources)

- Authorization is the process of verifying that you have access to something. Gaining access to a resource (e.g. directory on a hard disk) because the permissions configured on it allow you access is authorization.

Non-repudiation (also termed Accounting)

- Non-repudiation is the assurance that someone cannot deny something. Typically, non-repudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated

↓

Records have been logged

→ Cannot state IDK

Some Terms

Vulnerability — A weakness that is inherent in every networks, devices and applications. This includes routers, switches, desktops, servers, software, etc.

Threats — The people eager, willing, and qualified to take advantage of each security weakness, and they continually search for new exploits and weaknesses.

Attacks — The threats use a variety of tools, scripts, and programs to launch attacks against networks and network devices. Typically, the network devices under attack are the endpoints, such as servers and desktops.

What is the difference between an exploit and vulnerability?

- A **vulnerability** is a flaw in a system, or in some software in a system, that could provide an attacker with a way to bypass the security infrastructure of the host operating system or of the software itself. It isn't an open door but rather a weakness which if attacked could provide a way in.
- **Exploiting** is the act of trying to turn a vulnerability (a weakness) into an actual way to breach a system. A vulnerability can therefore be 'exploited' to turn it into viable method to attack a system.
- An **exploit** (from the English verb to exploit, meaning "to use something to one's own advantage") is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic (usually computerized). Such behavior frequently includes things like gaining control of a computer system, allowing privilege escalation, or a denial-of-service (DoS or related DDoS) attack. (Extracted from Wikipedia)

Types of Vulnerabilities

Technological Weaknesses (技術問題)

- Computer and network technologies have intrinsic security weaknesses. These include TCP/IP protocol weaknesses, operating system weaknesses, and network equipment weaknesses.

Configuration Weaknesses (設定問題)

- Common examples: unsecured user accounts, system accounts with easily guessed passwords, misconfigured internet services, unsecured default settings within products, misconfigured network equipment.

Security Policy Weaknesses (安全政策問題)

- The network can pose security risks to the network if users do not follow the security policy.

Types of Threats

Unstructured threats - Not organized and do not target a specific host, network, or organization (In a random way)

- Unstructured threats consist of mostly inexperienced individuals using easily available hacking tools such as shell scripts and password crackers.

Structured threats - Organized efforts to attack a specific target (Planned attack)

- Structured threats come from hackers who are more highly motivated and technically competent. These people know system vulnerabilities and can understand, develop, and use sophisticated hacking techniques to penetrate unsuspecting businesses.

External threats (Not in-org attacks)

- External threats can arise from individuals or organizations working outside of a company. They do not have authorized access to the computer systems or network. They work their way into a network mainly from the Internet.

Internal threats (In-org attacks)

- Internal threats occur when someone has authorized access to the network with either an account on a server or physical access to the network.

Types of Attacks

Reconnaissance Attacks (vulnerability scanning)

- Reconnaissance is the unauthorized discovery and mapping of systems, services, or vulnerabilities. It is also known as information gathering (or network scanning, vulnerability scanning). In most cases, it precedes an actual access or denial-of-service (DoS) attack.

Access Attacks

- System access is the ability for an unauthorized intruder to gain access to a device for which the intruder does not have an account or a password.

Denial of service Attacks

- Denial of service implies that an attacker disables or corrupts networks, systems, or services with the intent to deny services to intended users.

Attacks by Malicious Code - worms, viruses, Trojan horses, etc

- Malicious software is inserted onto a host to damage a system; corrupt a system; replicate itself; or deny services or access to networks, systems or services. They can also allow sensitive information to be copied or echoed to other systems.

Who needs computer security?

Governments:

- To safeguard military or diplomatic communications and to protect national interests.

Private sector:

- To protect sensitive information such as health and legal records, financial transactions, credit ratings.
- To protect information ownership.

Individuals:

- To protect sensitive information, and to protect an individual's privacy in the electronic world.
- Allow E-commerce, internet banking and so on.

Summary of Security Basic