Exploiting Software Vulnerabilities

Vulnerability Management and Assessment

Universidad Zaragoza
1542

Dept. of Computer Science and Systems Engineering
University of Zaragoza, Spain

Course 2023/2024

Master's Degree in Informatics Engineering

UNIVERSITY OF ZARAGOZA

Room A.02, Ada Byron building

Outline

1. Introduction
   - Vulnerabilities
   - Adversaries / attackers
2. Ethical concerns
3. Vulnerability Management and Assessment
4. Vulnerability Metrics

Outline

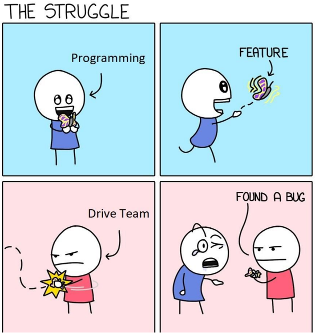
1 Introduction
- Vulnerabilities
- Adversaries / attackers

2 Ethical concerns

3 Vulnerability Management and Assessment

4 Vulnerability Metrics

Introduction



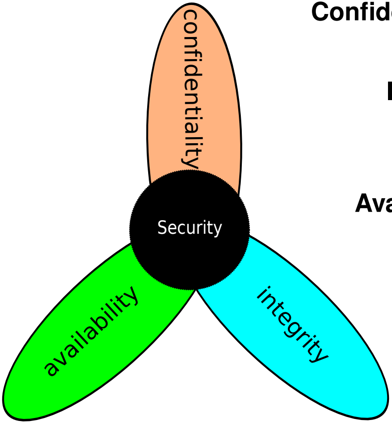
Definition of vulnerability

- **Software or design flaw**
- **Allows an intruder to reduce the security of information on a system**
- **Requirements**:
  - A weakness in the system
  - An adversary's access to that weakness
  - Ability of the adversary to exploit the weakness using a tool or a technique

Credits: https://www.reddit.com/r/FRC/comments/ay7tri/its_not_a_bug_its_a_feature/

Introduction

The CIA triad of infosec



Confidentiality *Information is not accessed by unauthorized people*

Integrity *Information is not altered by unauthorized people in way that is undetectable by authorized users*

Availability *Reliable (and timely) access and use of information, while avoiding unauthorized retention of information*

- **Other attributes**: authenticity, authorization, accountability, non-repudiation/anonymity

Introduction

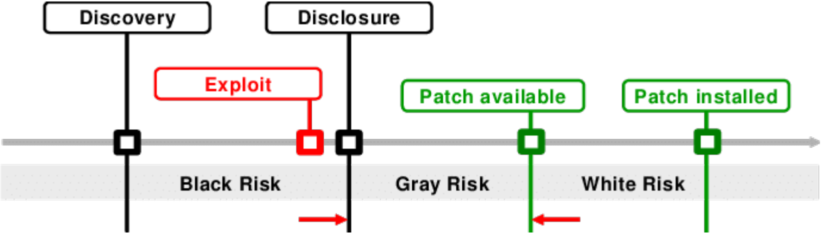
Security challenges

- **Lack of security awareness**
- **Sophistication of attack tools and methodologies**
  - Little or no knowledge or skill is required to carry out some attacks
  - Script-kiddies – *hackers de botón gordo*
- **Complexity of systems**
- **Growth of interconnected and heterogeneous devices** (e.g., IoT, ICS)
- **Lack of vulnerability/patch management processes**

There is **ALWAYS** a trade-off between security and usability

Introduction

Life-cycle of a vulnerability



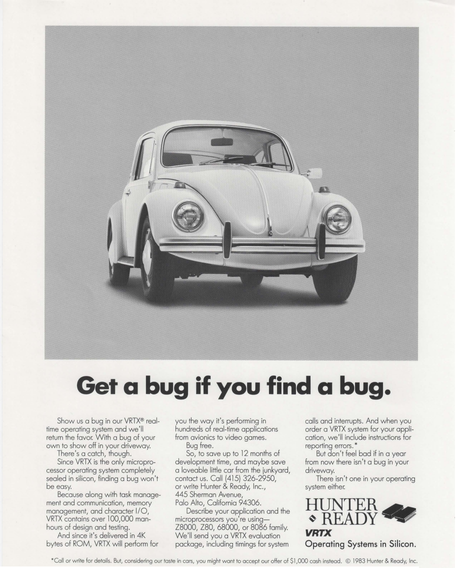
Zero-day vulnerability (0-day)

- **Unknown to the software vendor (and the public) until disclosed**

Credits: *0-Day Patch Exposing Vendors (In)security Performance*, S. Frei, B. Tellenbach, B. Plattner, BlackHat EU 2008

Introduction

Bug bounty programs



Get a bug if you find a bug.

Show us a bug in our VRTX® real-time operating system and we'll return the favor. With a bug of your own to show off in your driveway.

There's a catch, though.

Since VRTX is the only microprocessor operating system completely sealed in silicon, finding a bug won't be easy.

Because along with task management and communication, memory management, and character I/O, VRTX contains over 100,000 man-hours of design and testing.

And since it's delivered in 4K bytes of ROM, VRTX will perform for you the way it's performing in hundreds of real-time applications from avionics to video games.

Bug free.

So, to save up to 12 months of development time, and maybe save a loveable little car from the junkyard, contact us. Call (415) 326-2950, or write Hunter & Ready, Inc., 445 Sherman Avenue, Palo Alto, California 94306.

Describe your application and the microprocessors you're using—Z8000, Z80, 68000, or 8086 family. We'll send you a VRTX evaluation package, including timings for system calls and interrupts. And when you order a VRTX system for your application, we'll include instructions for reporting errors.*

But don't feel bad if in a year from now there isn't a bug in your driveway.

There isn't one in your operating system either.

HUNTER
READY
VRTX
Operating Systems in Silicon.

*Call or write for details. But, considering our taste in cars, you might want to accept our offer of $1,000 cash instead. © 1983 Hunter & Ready, Inc.

Further reading: *Bounties Mount for Bugs*, P. Marks, Communications of the ACM, Aug 2018.

Introduction

Types of vulnerability disclosures

- **Non-disclosure**
  - **Keep the vulnerability a secret** instead of contacting the software vendor or a computer security coordinating authority
  - **The number of undisclosed vulnerabilities is unknown**

Introduction

Types of vulnerability disclosures

- **Non-disclosure**
  - **Keep the vulnerability a secret** instead of contacting the software vendor or a computer security coordinating authority
  - **The number of undisclosed vulnerabilities is unknown**
- **Full disclosure**
  - **Inform the community at large**, without first consulting the software vendor
  - **Minimal documentation**: how it was found, the software products (with versions) affected, and how to exploit or mitigate it
  - **Controversial method**
    - Rapid recognition and patching of software vendors
    - Increase the risk of widespread exploitation

Introduction

Types of vulnerability disclosures

- **Non-disclosure**
  - **Keep the vulnerability a secret** instead of contacting the software vendor or a computer security coordinating authority
  - **The number of undisclosed vulnerabilities is unknown**
- **Full disclosure**
  - **Inform the community at large**, without first consulting the software vendor
  - **Minimal documentation**: how it was found, the software products (with versions) affected, and how to exploit or mitigate it
  - **Controversial method**
    - Rapid recognition and patching of software vendors
    - Increase the risk of widespread exploitation
- **Responsible disclosure** (aka partial/limited disclosure)
  - Usually accompanied by a **suite of tests to verify that future versions do not contain similar bugs**
  - **Inform the software vendor and wait for a response** (depends on their disclosure policy)
  - **If no response, go to full disclosure**

Introduction

What I have to do?

- **Contact a CERT/CC or the software vendor involved**
  - CERT/CC stands for Computer Emergency Response Team/Coordination Center
  - There are many CERTs (every country and large organization has one)
  - **Software vendors now provide direct communication with their security teams** to handle vulnerability discoveries
  - **Each CERT/vendor may have different disclosure policies**
  - **Industrial systems often have special disclosure processes**, due to their critical activity (e.g., `https://www.cisa.gov/coordinated-vulnerability-disclosure-process`)

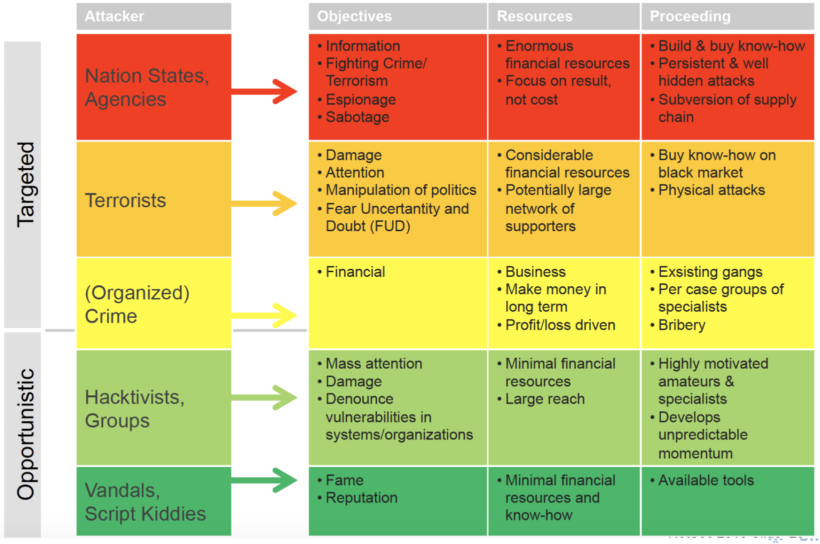
Introduction

What I have to do?

- **Contact a CERT/CC or the software vendor involved**
  - CERT/CC stands for Computer Emergency Response Team/Coordination Center
  - There are many CERTs (every country and large organization has one)
  - **Software vendors now provide direct communication with their security teams** to handle vulnerability discoveries
  - **Each CERT/vendor may have different disclosure policies**
  - **Industrial systems often have special disclosure processes**, due to their critical activity (e.g., `https://www.cisa.gov/coordinated-vulnerability-disclosure-process`)
- **Obtain a CVE** (Common Vulnerabilities and Exposures)
  - MITRE, ZDI, etc
  - Known syntax: CVE-YYYY-ID
    - *Example*: Zerologon vulnerability `https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1472`
  - **Useful to unambiguously identify a vulnerability**

Introduction

Actors and attackers



	Attacker	Objectives	Resources	Proceeding
Targeted	Nation States, Agencies	• Information • Fighting Crime/ Terrorism • Espionage • Sabotage	• Enormous financial resources • Focus on result, not cost	• Build & buy know-how • Persistent & well hidden attacks • Subversion of supply chain
	Terrorists	• Damage • Attention • Manipulation of politics • Fear Uncertantity and Doubt (FUD)	• Considerable financial resources • Potentially large network of supporters	• Buy know-how on black market • Physical attacks
	(Organized) Crime	• Financial	• Business • Make money in long term • Profit/loss driven	• Exsisting gangs • Per case groups of specialists • Bribery
Opportunistic	Hacktivists, Groups	• Mass attention • Damage • Denounce vulnerabilities in systems/organizations	• Minimal financial resources • Large reach	• Highly motivated amateurs & specialists • Develops unpredictable momentum
	Vandals, Script Kiddies	• Fame • Reputation	• Minimal financial resources and know-how	• Available tools

Credits: *(IN)SECURITY, RISK & THE LIFECYCLE OF VULNERABILITIES*, Dr. Stefan Frei, ETH

Introduction

Adversaries / attackers

- **Hacktivists**
  - **Individuals or hacker groups**
  - Primary motivation: **to promote a political agenda, religious belief, or social ideology**
- **Internal threats** (insiders)
  - **Current or former employees**. It can also arise from third parties (contractors, temporary workers, clients)
  - Different types: malicious, accidental, negligent
  - Primary motivation (of malicious insiders): **money, espionage, gain strategic advantage**
  - *Examples*: (taken from `https://www.varonis.com/blog/insider-threats/`)
    - At Tesla, a malicious insider sabotaged systems and sent proprietary data to third parties
    - At Facebook, a security engineer abused his access to harass women
    - At Coca-Cola, a malicious insider stole a hard drive full of worker's personal data
    - At Suntrust Bank, a malicious insider stole personal data (including account information) of 1.5M customers and provided it to a criminal organization

Introduction

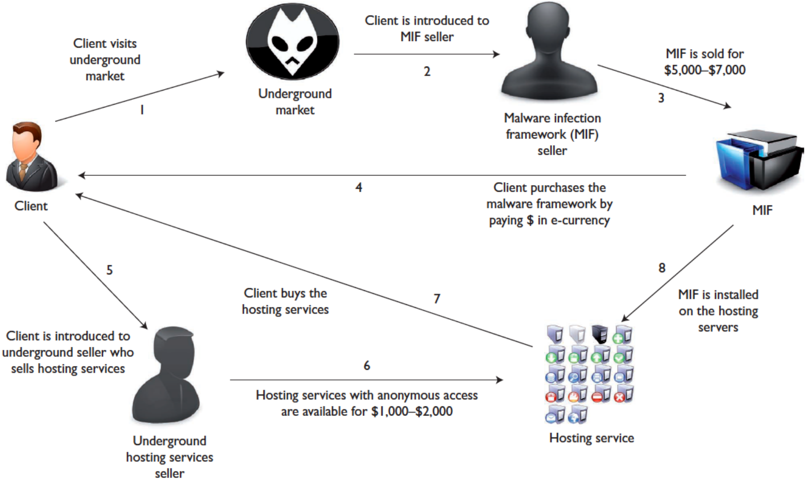
Adversaries / attackers

- **Cyber criminals** – *the traditional mafia moves to the digital world*
  - **Individuals or groups of people who use technology to commit cybercrimes**
  - Main motivation: **generate profits through different means** (theft of personal or confidential company data, sabotage, fraud, etc.)
  - **The most prominent and active type of attacker**
- **State-sponsored attackers**
  - Individuals or groups of people who have **particular objectives aligned with the political, commercial, or military interests of their country of origin**
  - **Highly trained hackers**, specialized in detecting and exploiting vulnerabilities
  - **Most dangerous attacker**: no resource limit

Further reading: *Cyber Guerilla*, Jelle van Haaster, Rickey Gevers and Martijn Sprengers, Syngress, 2016

Introduction

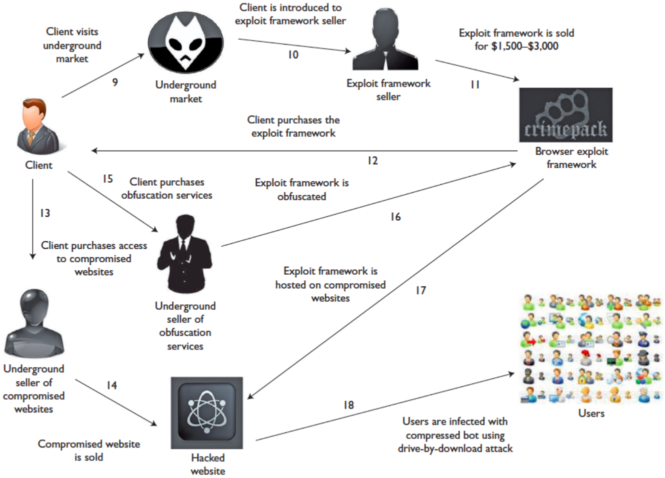
Cybercrime lifecycle – cycle 1


Client visits underground market
1
Underground market
Client is introduced to MIF seller
2
Malware infection framework (MIF) seller
MIF is sold for $5,000–$7,000
3
MIF
Client
4
Client purchases the malware framework by paying $ in e-currency
5
Client is introduced to underground seller who sells hosting services
Underground hosting services seller
Client buys the hosting services
7
6
Hosting services with anonymous access are available for $1,000–$2,000
Hosting service
8
MIF is installed on the hosting servers

Credits: Sood, A. K.; Bansal, R. & Enbody, R. J. *Cybercrime: Dissecting the State of Underground Enterprise*. IEEE Internet Computing, 2013, 17, 60–68.

Introduction

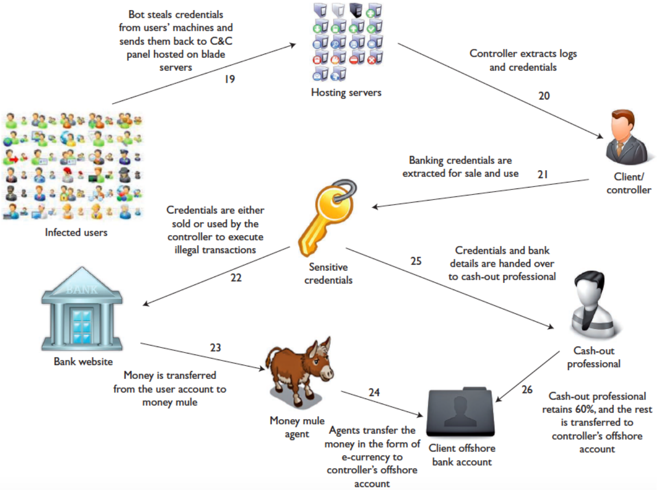
Cybercrime lifecycle – cycle 2


Client visits underground market
9
Underground market
Client is introduced to exploit framework seller
10
Exploit framework seller
Exploit framework is sold for $1,500–$3,000
11
crimepack
Browser exploit framework
Client purchases the exploit framework
12
Client
15
Client purchases obfuscation services
Exploit framework is obfuscated
16
13
Client purchases access to compromised websites
Underground seller of obfuscation services
Exploit framework is hosted on compromised websites
17
Underground seller of compromised websites
14
Compromised website is sold
Hacked website
18
Users are infected with compressed bot using drive-by-download attack
Users

Credits: Sood, A. K.; Bansal, R. & Enbody, R. J. *Cybercrime: Dissecting the State of Underground Enterprise*. IEEE Internet Computing, 2013, 17, 60–68.

Introduction

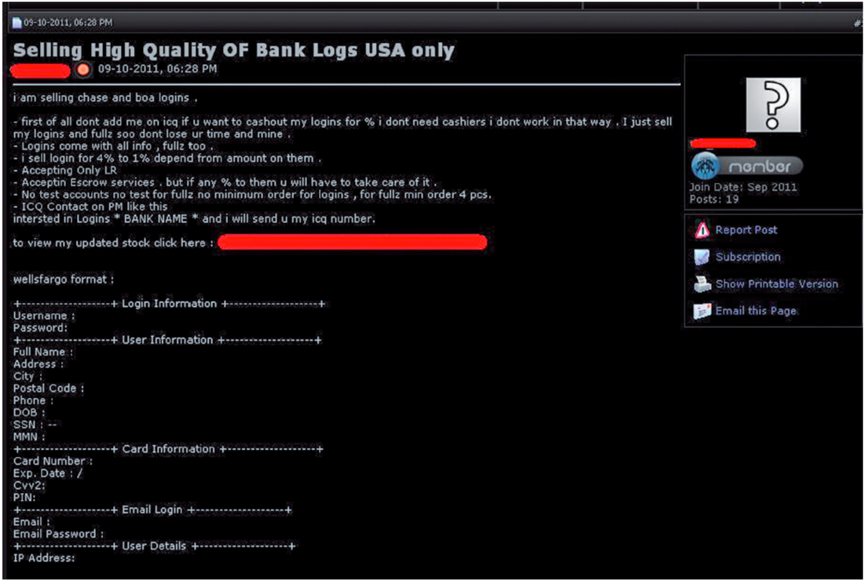
Cybercrime lifecycle – cycle 3


Bot steals credentials from users' machines and sends them back to C&C panel hosted on blade servers
19
Hosting servers
Controller extracts logs and credentials
20
Client/ controller
Infected users
Banking credentials are extracted for sale and use
21
Credentials are either sold or used by the controller to execute illegal transactions
Sensitive credentials
22
25
Credentials and bank details are handed over to cash-out professional
BANK
Bank website
23
Money is transferred from the user account to money mule
Cash-out professional
Money mule agent
24
Agents transfer the money in the form of e-currency to controller's offshore account
Client offshore bank account
26
Cash-out professional retains 60%, and the rest is transferred to controller's offshore account

Credits: Sood, A. K.; Bansal, R. & Enbody, R. J. *Cybercrime: Dissecting the State of Underground Enterprise.* IEEE Internet Computing, 2013, 17, 60–68.

Introduction

Some examples about the underground market



09-10-2011, 06:28 PM

Selling High Quality OF Bank Logs USA only

[redacted] 09-10-2011, 06:28 PM

i am selling chase and boa logins .

- first of all dont add me on icq if u want to cashout my logins for % i dont need cashiers i dont work in that way . I just sell my logins and fullz soo dont lose ur time and mine .
- Logins come with all info , fullz too .
- i sell login for 4% to 1% depend from amount on them .
- Accepting Only LR
- Acceptin Escrow services . but if any % to them u will have to take care of it .
- No test accounts no test for fullz no minimum order for logins , for fullz min order 4 pcs.
- ICQ Contact on PM like this

interted in Logins * BANK NAME * and i will send u my icq number.

to view my updated stock click here : [redacted]

wellsfargo format :

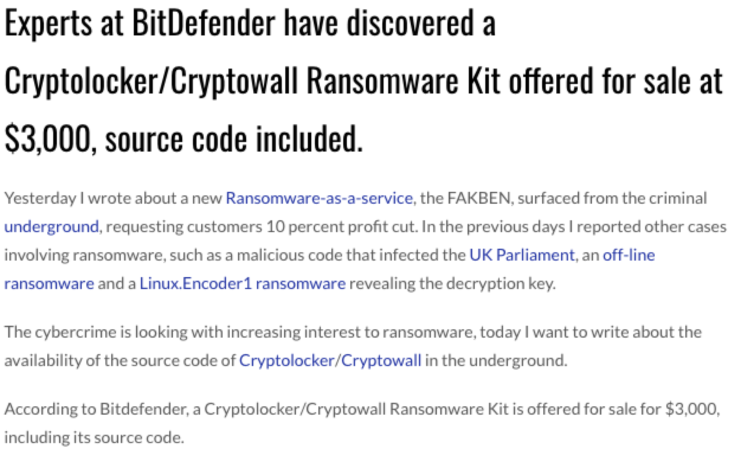
```
+------------------+ Login Information +------------------+
Username :
Password:
+------------------+ User Information +------------------+
Full Name :
Address :
City :
Postal Code :
Phone :
DOB :
SSN : --
MMN :
+------------------+ Card Information +------------------+
Card Number :
Exp. Date : /
Cvv2:
PIN:
+------------------+ Email Login +------------------+
Email :
Email Password :
+------------------+ User Details +------------------+
IP Address:
```

[redacted]

Join Date: Sep 2011
Posts: 19

Introduction

Some examples about the underground market



Experts at BitDefender have discovered a Cryptolocker/Cryptowall Ransomware Kit offered for sale at $3,000, source code included.

Yesterday I wrote about a new Ransomware-as-a-service, the FAKBEN, surfaced from the criminal underground, requesting customers 10 percent profit cut. In the previous days I reported other cases involving ransomware, such as a malicious code that infected the UK Parliament, an off-line ransomware and a Linux.Encoder1 ransomware revealing the decryption key.

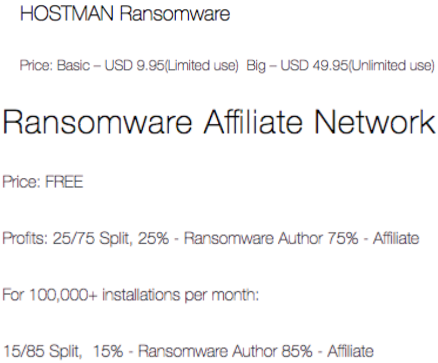
The cybercrime is looking with increasing interest to ransomware, today I want to write about the availability of the source code of Cryptolocker/Cryptowall in the underground.

According to Bitdefender, a Cryptolocker/Cryptowall Ransomware Kit is offered for sale for $3,000, including its source code.

Credits: `http://securityaffairs.co/wordpress/41977/cyber-crime/ransomware-kit-for-sale.html`

Introduction

Some examples about the underground market



HOSTMAN Ransomware

Price: Basic – USD 9.95(Limited use) Big – USD 49.95(Unlimited use)

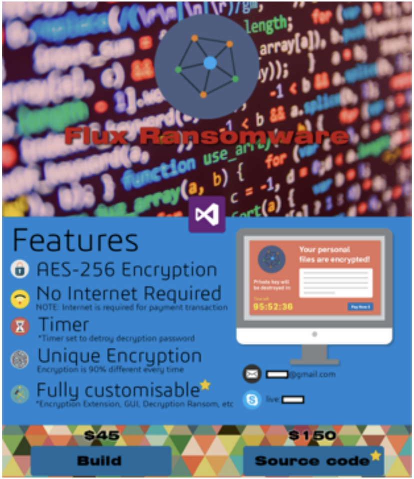
Ransomware Affiliate Network

Price: FREE

Profits: 25/75 Split, 25% - Ransomware Author 75% - Affiliate

For 100,000+ installations per month:

15/85 Split, 15% - Ransomware Author 85% - Affiliate



Features

- AES-256 Encryption
- No Internet Required
  NOTE: Internet is required for payment transaction
- Timer
  *Timer set to detroy decryption password
- Unique Encryption
  Encryption is 90% different every time
- Fully customisable
  *Encryption Extension, GUI, Decryption Ransom, etc

Your personal files are encrypted!
Private key will be destroyed in:
Time left
95:52:36
Pay Now

[redacted]@gmail.com

live:[redacted]

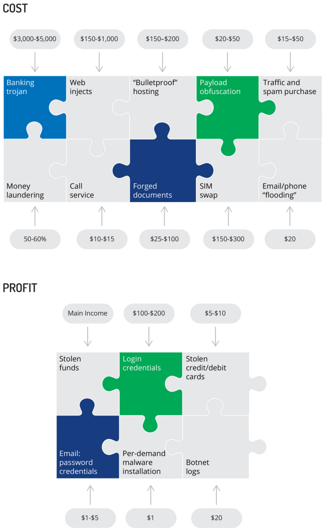
$45 Build

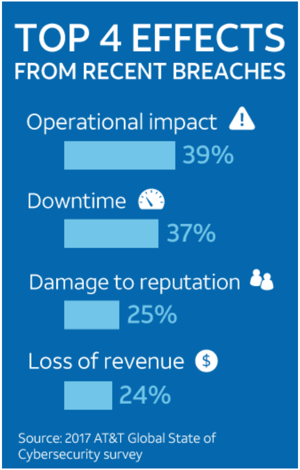
$150 Source code

Credits: https://blog.fortinet.com/

Introduction

Estimating the costs and benefits of cybercrime (2017)



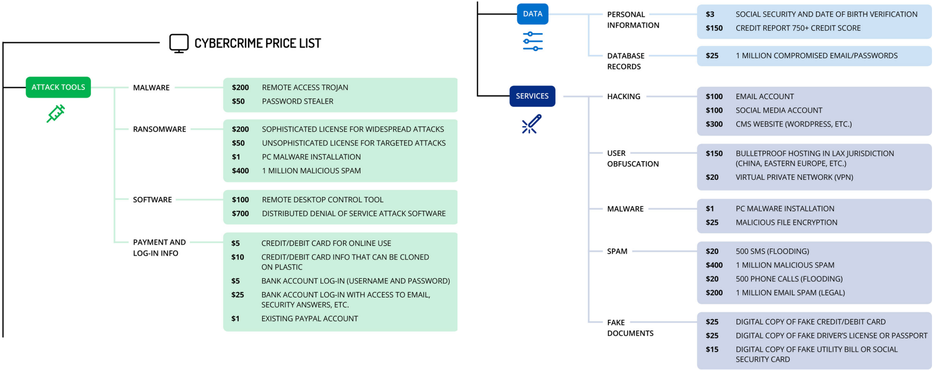


Source: 2017 AT&T Global State of Cybersecurity survey

Credits: https://www.recordedfuture.com/cyber-operations-cost/

Introduction

Let’s go shopping, folks! (2017)



CYBERCRIME PRICE LIST

ATTACK TOOLS

MALWARE	$200	REMOTE ACCESS TROJAN
	$50	PASSWORD STEALER
RANSOMWARE	$200	SOPHISTICATED LICENSE FOR WIDESPREAD ATTACKS
	$50	UNSOPHISTICATED LICENSE FOR TARGETED ATTACKS
	$1	PC MALWARE INSTALLATION
	$400	1 MILLION MALICIOUS SPAM
SOFTWARE	$100	REMOTE DESKTOP CONTROL TOOL
	$700	DISTRIBUTED DENIAL OF SERVICE ATTACK SOFTWARE
PAYMENT AND LOG-IN INFO	$5	CREDIT/DEBIT CARD FOR ONLINE USE
	$10	CREDIT/DEBIT CARD INFO THAT CAN BE CLONED ON PLASTIC
	$5	BANK ACCOUNT LOG-IN (USERNAME AND PASSWORD)
	$25	BANK ACCOUNT LOG-IN WITH ACCESS TO EMAIL, SECURITY ANSWERS, ETC.
	$1	EXISTING PAYPAL ACCOUNT

DATA

PERSONAL INFORMATION	$3	SOCIAL SECURITY AND DATE OF BIRTH VERIFICATION
	$150	CREDIT REPORT 750+ CREDIT SCORE
DATABASE RECORDS	$25	1 MILLION COMPROMISED EMAIL/PASSWORDS

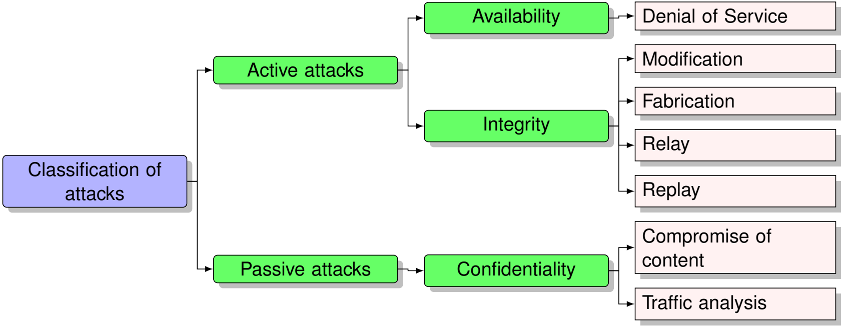
SERVICES

HACKING	$100	EMAIL ACCOUNT
	$100	SOCIAL MEDIA ACCOUNT
	$300	CMS WEBSITE (WORDPRESS, ETC.)
USER OBFUSCATION	$150	BULLETPROOF HOSTING IN LAX JURISDICTION (CHINA, EASTERN EUROPE, ETC.)
	$20	VIRTUAL PRIVATE NETWORK (VPN)
MALWARE	$1	PC MALWARE INSTALLATION
	$25	MALICIOUS FILE ENCRYPTION
SPAM	$20	500 SMS (FLOODING)
	$400	1 MILLION MALICIOUS SPAM
	$20	500 PHONE CALLS (FLOODING)
	$200	1 MILLION EMAIL SPAM (LEGAL)
FAKE DOCUMENTS	$25	DIGITAL COPY OF FAKE CREDIT/DEBIT CARD
	$25	DIGITAL COPY OF FAKE DRIVER’S LICENSE OR PASSPORT
	$15	DIGITAL COPY OF FAKE UTILITY BILL OR SOCIAL SECURITY CARD

Credits: `https://www.recordedfuture.com/cyber-operations-cost/`

Introduction

Classification of attacks



Credits: adapted from *(IN)SECURITY, RISK & THE LIFECYCLE OF VULNERABILITIES*, Dr. Stefan Frei, ETH

Outline

1 Introduction

2 Ethical concerns

3 Vulnerability Management and Assessment

4 Vulnerability Metrics

Ethical concerns

Vulnerability research

- *Some concerns...*
  - We are testing systems and analyzing products created and maintained by someone else
  - **But we help others prevent or mitigate harm to third parties due to vulnerable products and operations...**

Ethical concerns

Vulnerability research

- *Some concerns...*
  - We are testing systems and analyzing products created and maintained by someone else
  - **But we help others prevent or mitigate harm to third parties due to vulnerable products and operations...**
- *What about legality?*
  - State and federal computer intrusion statutes or intellectual property rights are violated
  - **But vulnerability research helps us anticipate the problems...**
  - When the disclosure is legally required, irreparable harm has usually been done

Ethical concerns

Code of conduct

- **Duty to do no harm**
- *Before you start your research...*
  - **Reveal intent and investigation**
  - **Seek legal advice**
- *During and after your research...*
  - **Responsible data management**
  - **Report serious vulnerabilities**

Outline

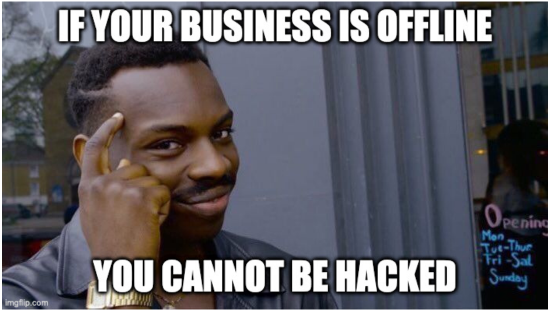
1 Introduction

2 Ethical concerns

3 Vulnerability Management and Assessment

4 Vulnerability Metrics

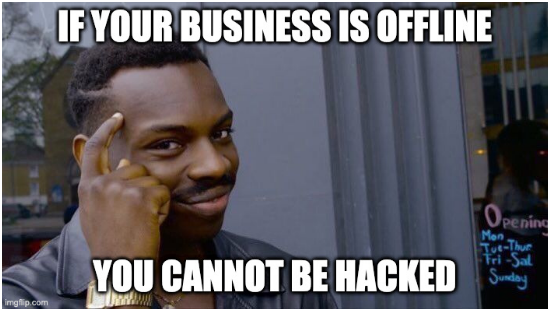
Vulnerability Management and Assessment



Absolute security does not exist

- **There are always trade-offs**: usability, social, financial, etc...
- TAKE-HOME MESSAGE: **the correct security metric is RONI** (Return Of Non Investment)
  - *You cannot calculate the return on your security spending, but you can calculate your loss from not investing in security after an incident occurs*

Vulnerability Management and Assessment



Absolute security does not exist

- **There are always trade-offs**: usability, social, financial, etc...
- TAKE-HOME MESSAGE : **the correct security metric is RONI** (Return Of Non Investment)
  - *You cannot calculate the return on your security spending, but you can calculate your loss from not investing in security after an incident occurs*

What are you willing to give up to get the level of security you want?

- **Vulnerability management helps make decisions**

Vulnerability Management and Assessment

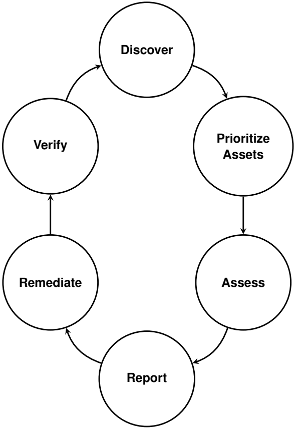
Vulnerability management

- **Identification of vulnerabilities in systems**
- **Risk assessment associated with these vulnerabilities**

Vulnerability Management and Assessment

Vulnerability management

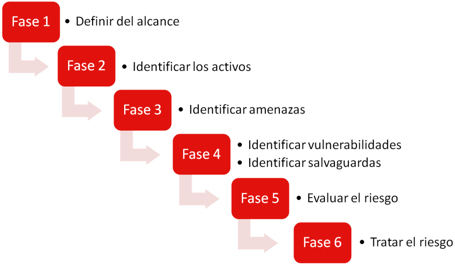
- **Identification of vulnerabilities in systems**
- **Risk assessment associated with these vulnerabilities**



- **Discover**: inventory all assets and identify vulnerabilities
- **Prioritize assets**: categorize assets into groups, assigning a value based on their importance for the operation of your business
- **Assess**: determine a baseline risk profile
- **Report**: measure the level of risk associated with assets, in accordance with the current security policies
- **Remediate**: prioritize and fix vulnerabilities
- **Verify**: audit the system to verify that threats no longer exist

Vulnerability Management and Assessment

Risk analysis process



Fase 1
- Definir del alcance

Fase 2
- Identificar los activos

Fase 3
- Identificar amenazas

Fase 4
- Identificar vulnerabilidades
- Identificar salvaguardas

Fase 5
- Evaluar el riesgo

Fase 6
- Tratar el riesgo

- **Identify threats.** The use of standard methodologies such as MAGERIT v3 can help (see `https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html`)
- **Manage risk.** Four possibilities:
  - *Transfer the risk to a third-party* (i.e., purchase insurance)
  - *Avoid the risk*
  - *Accept the risk* (be careful with this)
  - *Mitigate (reduce) the risk*

Credits: `https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo`

Vulnerability Management and Assessment

Vulnerability assessment

- **Systematic review of security weaknesses in a system**
- **Assess the system for known vulnerabilities, prioritize them, and recommend action** (transfer, remediation, mitigation, avoidance)

Vulnerability Management and Assessment

Vulnerability assessment

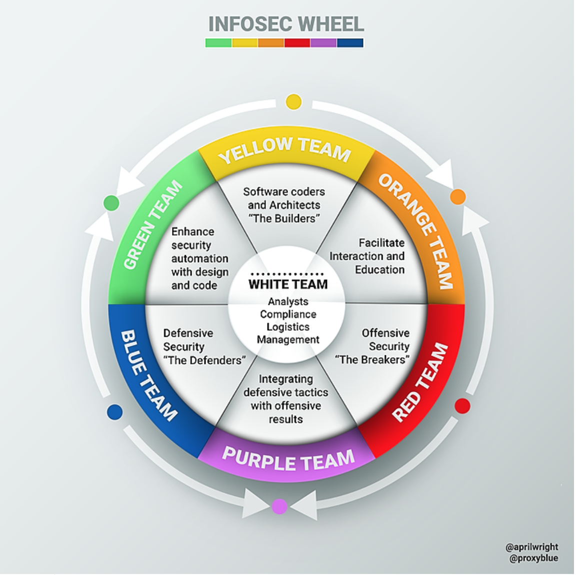
- **Systematic review of security weaknesses in a system**
- **Assess the system for known vulnerabilities, prioritize them, and recommend action** (transfer, remediation, mitigation, avoidance)

Types of assessments

- **External analysis**: focused on components accessible to external users
- **Internal scans**: any system component on the internal network (not exposed to external users)
- **Environmental scans**: focused on specific operational technologies used by the organization (e.g., cloud services, mobile devices, etc.)

Vulnerability Management and Assessment

Red, blue, and... even purple?



INFOSEC WHEEL
YELLOW TEAM
Software coders and Architects "The Builders"
ORANGE TEAM
Facilitate Interaction and Education
RED TEAM
Offensive Security "The Breakers"
PURPLE TEAM
Integrating defensive tactics with offensive results
BLUE TEAM
Defensive Security "The Defenders"
GREEN TEAM
Enhance security automation with design and code
WHITE TEAM
Analysts
Compliance
Logistics
Management
@aprilwright
@proxyblue

Credits: https://hackernoon.com/

Vulnerability Management and Assessment

Vulnerability assessment reports

- **The shorter, the better: get straight to the point**
- Aimed at the management and security staff of an organization
- **Typical structure**:
  - Executive summary
  - Introduction: scope, extent and limitations
  - Laws, regulations, and policies
  - Identification of assets
  - Threat assessment
  - Audit process
  - Summary

Outline

1 Introduction

2 Ethical concerns

3 Vulnerability Management and Assessment

4 Vulnerability Metrics

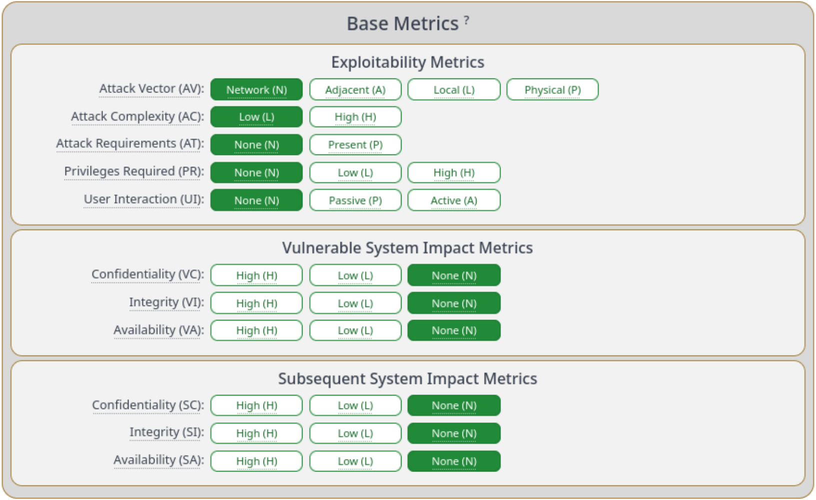
Vulnerability Metrics

Common Vulnerability Scoring System (CVSS)

- **Metric to assess the criticality of vulnerabilities**
- Internationally recognized and tested for years
- **Three groups of metrics**
  - **Base Metric Group**
  - **Temporal Metric Group**
  - **Environmental Metric Group**
- **Proposed by FIRST**
  - "[Joint] incident response and security teams from every country across the world to ensure a safe internet for all"
- **Online calculator**: `https://www.first.org/cvss/calculator/4.0`

Vulnerability Metrics

CVSS v4.0



Base Metrics ?

Exploitability Metrics

Attack Vector (AV): [✓ Network (N)] Adjacent (A) Local (L) Physical (P)

Attack Complexity (AC): [✓ Low (L)] High (H)

Attack Requirements (AT): [✓ None (N)] Present (P)

Privileges Required (PR): [✓ None (N)] Low (L) High (H)

User Interaction (UI): [✓ None (N)] Passive (P) Active (A)

Vulnerable System Impact Metrics

Confidentiality (VC): High (H) Low (L) [✓ None (N)]

Integrity (VI): High (H) Low (L) [✓ None (N)]

Availability (VA): High (H) Low (L) [✓ None (N)]

Subsequent System Impact Metrics

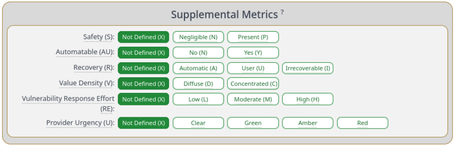
Confidentiality (SC): High (H) Low (L) [✓ None (N)]

Integrity (SI): High (H) Low (L) [✓ None (N)]

Availability (SA): High (H) Low (L) [✓ None (N)]

Vulnerability Metrics

CVSS v4.0

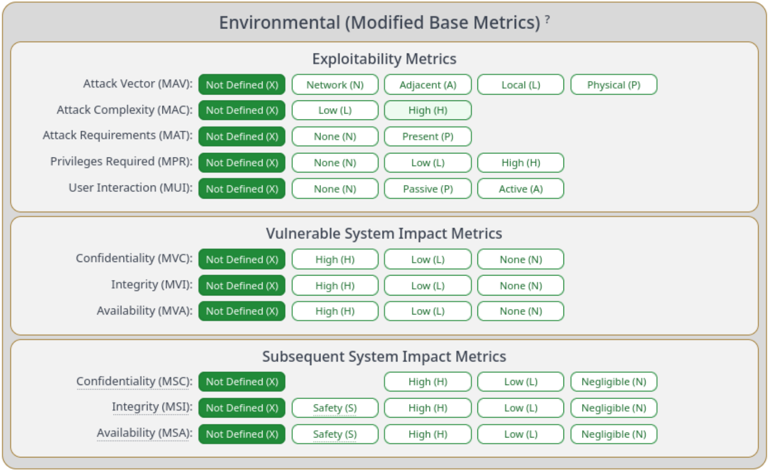


Supplemental Metrics ?

Safety (S):	[✓ Not Defined (X)]	Negligible (N)	Present (P)		
Automatable (AU):	[✓ Not Defined (X)]	No (N)	Yes (Y)		
Recovery (R):	[✓ Not Defined (X)]	Automatic (A)	User (U)	Irrecoverable (I)	
Value Density (V):	[✓ Not Defined (X)]	Diffuse (D)	Concentrated (C)		
Vulnerability Response Effort (RE):	[✓ Not Defined (X)]	Low (L)	Moderate (M)	High (H)	
Provider Urgency (U):	[✓ Not Defined (X)]	Clear	Green	Amber	Red

Vulnerability Metrics

CVSS v4.0



Environmental (Modified Base Metrics) ?

Exploitability Metrics

Attack Vector (MAV):	Not Defined (X)	Network (N)	Adjacent (A)	Local (L)	Physical (P)
Attack Complexity (MAC):	Not Defined (X)	Low (L)	High (H)		
Attack Requirements (MAT):	Not Defined (X)	None (N)	Present (P)		
Privileges Required (MPR):	Not Defined (X)	None (N)	Low (L)	High (H)	
User Interaction (MUI):	Not Defined (X)	None (N)	Passive (P)	Active (A)	

Vulnerable System Impact Metrics

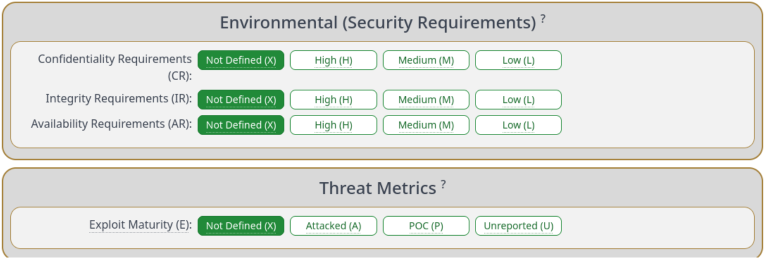
Confidentiality (MVC):	Not Defined (X)	High (H)	Low (L)	None (N)
Integrity (MVI):	Not Defined (X)	High (H)	Low (L)	None (N)
Availability (MVA):	Not Defined (X)	High (H)	Low (L)	None (N)

Subsequent System Impact Metrics

Confidentiality (MSC):	Not Defined (X)		High (H)	Low (L)	Negligible (N)
Integrity (MSI):	Not Defined (X)	Safety (S)	High (H)	Low (L)	Negligible (N)
Availability (MSA):	Not Defined (X)	Safety (S)	High (H)	Low (L)	Negligible (N)

Vulnerability Metrics

CVSS v4.0



Environmental (Security Requirements) ?

Confidentiality Requirements (CR): ● Not Defined (X) ○ High (H) ○ Medium (M) ○ Low (L)

Integrity Requirements (IR): ● Not Defined (X) ○ High (H) ○ Medium (M) ○ Low (L)

Availability Requirements (AR): ● Not Defined (X) ○ High (H) ○ Medium (M) ○ Low (L)

Threat Metrics ?

Exploit Maturity (E): ● Not Defined (X) ○ Attacked (A) ○ POC (P) ○ Unreported (U)

Vulnerability Metrics

CVSS v4.0

- **Qualitative criteria severity rating scale** since version 3.0
- Good for prioritizing vulnerabilities (as part of vulnerability assessment)

Score	Severity
0	None
$[0.1, 3.9]$	Low
$[4.0, 6.9]$	Medium
$[7.0, 8.9]$	High
$[9.0, 10]$	Critical

Exploiting Software Vulnerabilities

Vulnerability Management and Assessment

Universidad Zaragoza
1542

Dept. of Computer Science and Systems Engineering
University of Zaragoza, Spain

Course 2023/2024

Master's Degree in Informatics Engineering

UNIVERSITY OF ZARAGOZA

Room A.02, Ada Byron building