

Cyber Threat
Intelligence:
Dark Web

TABLE OF CONTENTS

Introduction 3

 Threat Intelligence on the Dark Web 3

The Underground Economy of Cybercrime..... 4

 Products, Services and Actor Roles 4

Security strategies for preventing data compromise 11

 Identify and classify sensitive data 11

 Access control lists 11

 Data Encryption 12

 Best Practices for Systems Hardening 13

 Cyber Security Awareness 13

Definitions 14

Analist Arda Büyükkaya

Cyber Threat Intelligence: Dark Web Report

Introduction

Cyber Threat Intelligence (CTI), focuses on data collection and information analysis so that we can gain a better understanding of the threats facing an organization. This helps us protect its assets. The objective of any CTI analyst is to produce and deliver relevant, accurate, and timely curated information, that is, intelligence so that the recipient organization can learn how to protect itself from a potential threat.

Threat Intelligence on the Dark Web

The amount of information on Underground forums and marketplaces is enormous, filtering this raw data and creating actionable items to protect Governments or Companies are the key achievement for us. Cybercriminals using Dark Web (Onion routing) for Privacy purposes, Social Networking, Stack Exchange and as a marketplace.



Figure 1 The intelligence cycle

“Intelligence is a corporate capability to forecast change in time to do something about it. The capability involves foresight and insight, and is intended to identify impending change, which may be positive, representing opportunity, or negative, representing threat.”

The Underground Economy of Cybercrime

The cybercrime underground maintains its own economy by easy to use products and services. Financial transactions have been increased with accessibility of anonymous cryptocurrencies such as Bitcoin, which is commonly used by malicious actors amongst themselves as well as for accepting payments from victims (e.g., ransomware).

Ransomware attacks are on the rise, but the question is, how could a group of cyber criminals compromise thousands of computers from various companies? Short answer is; underground markets being used by these Ransomware Groups to buy remote access on multiple victims, these remote access sellers are called Initial Access Brokers.

According to Small Business Innovation Research (SBIR) “Cybercrime costs the global economy about \$445 billion every year, with the damage to business from theft of intellectual property exceeding the \$160 billion loss to individuals. Cybercrime is becoming a growing and significant concern for small businesses.”

Products, Services and Actor Roles

The services offered within the cybercrime economy utilizes a leasing structure, in which access to a product is promised at a set rate for a fixed period of time. The sellers benefit from a guaranteed source of recurrent revenue throughout an extended period of time, and buyers benefit from the continued availability and performance of malicious tools

Products can be broken down into two main categories: information and resources

Stolen personally identifiable information (PII): Including everything from mass email lists used by spammers to full identity theft packages to commit financial fraud

Exfiltrated organizational information: Including intellectual capital / property, non-public internal data, and internal operational details

Harvested authentication credentials: Stolen username and password combinations continue to present a significant risk these days, especially when those credentials are re-used across multiple sites

USA phones database - 183,000,000+ lines By NetSec, May 1	7 replies 1131 views	C	Classymax 22 hours ago
USA FULLZ SSN+DOB 4kk By kalipso_0, July 12	1 reply 394 views	C	Classymax 22 hours ago
Forex Germany 106K Records By cypherdecoder, yesterday at 10:34 AM	0 replies 85 views	C	cypherdecoder Yesterday at 10:34 AM
Germany ebay orders and Belgium LinkedIn DATABASE By MasterBolo, July 2	6 replies 715 views	M	MasterBolo July 13
Sweden Gambling List Database and Ireland 2022 FULL INFO By MasterBolo, June 29	4 replies 705 views	M	MasterBolo July 13
bestblackhatforum.com 267k user database By gero, Monday at 04:36 PM	6 replies 324 views	gero	gero Tuesday at 06:34 PM
Giveaway - US Fullz By secure, Tuesday at 12:36 AM	3 replies 203 views	S	secure Tuesday at 05:54 PM
Валидные админки с правами администратора By locatve, Sunday at 10:00 PM	2 replies 288 views	locat	locatve Tuesday at 03:32 PM
LovePlanet.ru search for db By John_Malkovich, April 19, 2021	22 replies 2057 views	C	colo8585 Tuesday at 03:23 PM
ETFinance.eu 44K 2021 By cypherdecoder, Tuesday at 12:20 PM	0 replies 123 views	C	cypherdecoder Tuesday at 12:20 PM
Forex FxTraders 693k Records 2021 By cypherdecoder, Tuesday at 12:16 PM	0 replies 114 views	C	cypherdecoder Tuesday at 12:16 PM

Pilfered financial / Payment data: Unauthorized withdrawals from accounts or charges against credit lines continue to plague account holders

Buying CVV / Dumps - bulk/shop vendor - 60k buyers base
By easydeals, August 14, 2021 in [Finance] - billing, banks, accounts, logs

easydeals
byte

Seller
14 posts
Joined 08/13/21 (ID: 119025)
Activity другое / other
Deposit 0.060499 \$

Posted August 14, 2021 (edited)

Oldest shop in the market looking for suppliers.

**Over 60 000 buyers base, 10 000 daily active buyers.
Network of shops connected to our platform.**

1. Highest selling prices to secure good quality for our buyers.
2. High suppliers share - between 60% and 80%.
3. Fast payout: max 24 hours from payout request for minimum 500\$ payout.
4. Automatic seller panel with all the information to control sales and see refunds.
5. 24 hours No Refund for buyers, when new bases are posted and valid rate is over 70%.
6. Pre-Order system to increase top bins prices.
7. Also buying in BULK with forum escrow.

Shop domains: easydeals.ec or easydeals.gs.

PM for more details and jabber contact. Contact also directly in shop on ticket.

Thank you!

Figure 2 Selling CVV data

Resource products include elements such as:

Access to feature-rich malware:

Malware across varying capabilities (e.g., information stealers, remote administration tools – RATs, ransomware, purpose built utilities) that demonstrate consistent results and avoid source code leakage can generate significant revenue for associated authors and distributors

Crux kilobyte
 Posted April 2, 2021 (edited)

MemPOS scans for dumps (T1/T2) and CVVs stored in memory, files, keyboard, clipboard or network packets in several different known formats by utilizing algorithms and a series of handpicked Regex. All traffic is encrypted with SSL and transported via the Tor network to your own hidden service (.onion address), which we can assist in setting up for you in less than 2 minutes. It's a **guarantee** that **MemPOS** performs better than any other existing POS malware. Best of all, it is extremely easy to setup and getting started with.

Demonstration:
<https://www.youtube.com/watch?v=ZSSLVGy3Tlo>

MemPOS catches dumps and CVVs by means of:

- * Continuously scanning memory space of **x86** and **x64** bits processes
- * Continuously scanning relevant files on all connected drives and caching those for less redundancy
- * Monitoring network packets from active interfaces
- * Monitoring clipboard for data transmissions
- * Monitoring keyboard interfaces, which is especially effective against certain POS software utilizing this method

Bot features:

- * Low profile: Utilizes process affinity for minimal CPU load. Typically using a single core only and averages about < 1% of CPU load.
- * Hidden+Normal startup methods
- * Process persistence (automatically re-spawn process if killed)
- * Utilizing hashing of dumps/CVVs and scanned memory blocks to avoid redundancy
- * Reports to panel every minute

Panel features:

- * Bot info shown is ID, HWID, IP/LAN, PC/User, OS, Install date, Last seen, Dumps/Tracks, CVVs, Relapse, CPU usage
- * Guest account for allowing trusted partners to view statistics and masking sensitive details (dumps/CVVs)
- * Export dumps or CVVs with customizable details like selecting columns and delimiters
- * Relapse level - View ratio of returning customers in % for each POS system
- * Marking dumps or CVVs as sold
- * Daily statistics chart
- * Download and execute
- * Clear tracks/cvvs
- * Delete bot

Figure 3 MemPOS - POS/Cvv Malware

Bot features

- Utilizes process affinity for minimal CPU load
- Low profile with respect to CPU and memory load
- Hidden+Normal startup methods
- Process persistence (automatically re-spawn process if killed)
- Utilizing hashing of dumps/CVVs and scanned memory blocks to avoid redundancy
- Reports to panel every minute

Panel features

- Bot info shown is ID, HWID, IP/LAN, PC/User, OS, Install date, Last seen, Dumps/Tracks, CVVs, Relapse, CPU usage
- Guest account for allowing trusted partners to view statistics and masking sensitive details (dumps/CVVs)
- Export dumps or CVVs with customizable details like selecting columns and delimiters
- Relapse level - View ratio of returning customers in % for each POS system
- Marking dumps or CVVs as sold
- Daily statistics chart
- Download and execute
- Clear tracks/cvvs
- Delete bot

Lifetime License
\$500 USD
 PURCHASE NOW

MONERO Bitcoin

MemPOS is coded in C# .NET and has been extensively tested with various POS systems for long periods with excellent results.

MemPOS utilizes process affinity for minimal CPU load.

It automatically saves and prioritize processes it has found relevant data from for faster and focused scans in order to beat certain POS systems known for quickly wiping their memory space.

Figure 4 Advertisement of MemPOS Malware

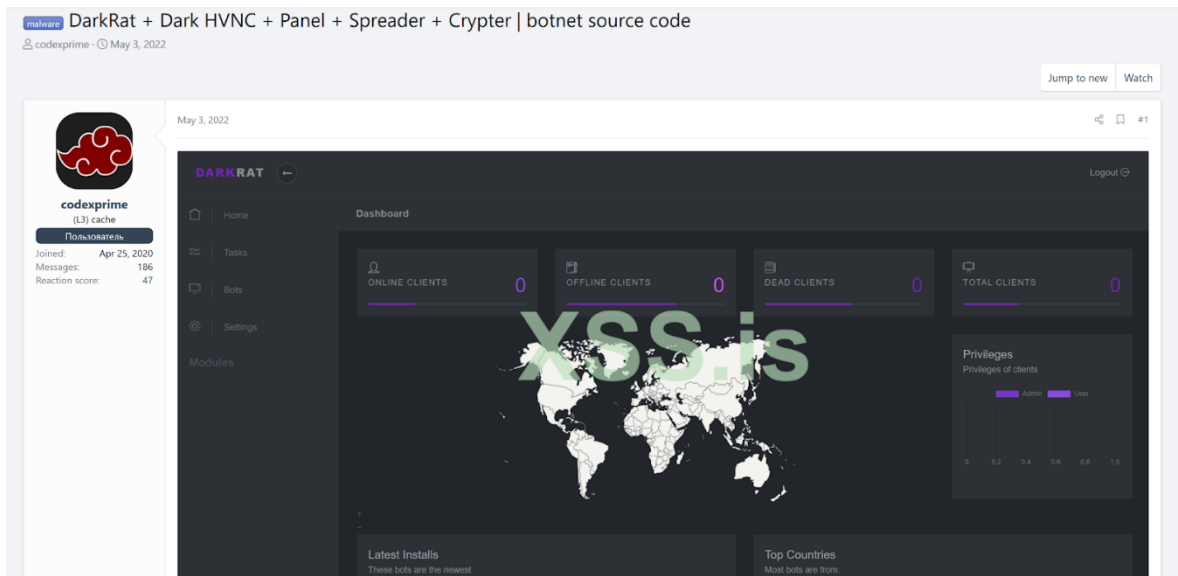



Figure 5 Source code leakage of Dark Rat

Ransomware actors wanted to get Initial Access on corporate networks without being detected by EDR/AVs, oftentimes 0-day exploits may be so expensive to achieve that so they can use private malware loaders for evading the detection.

Solmyr
gigabyte
●●●●



Seller
12
167 posts
Joined
08/06/19 (ID: 94865)
Activity
вирусология / malware
Deposit
0.2025 ₮

Posted July 28, 2021

Welcome to my sales thread.

Product: [XLL Excel Dropper](#)

Type: One click

XLL dropper is a great alternative to Macros and 1-day silent exploits. Upon opening, the XLL file will display a popup. It only takes one click on the popup to execute your file. (see video below!)

Features:

- **Full Coverage**
This XLL dropper works on patched and unpatched office.
Supported office versions: 2003, 2007, 2010, 2013, 2016, 2019, office365
Supported Windows versions: XP, Vista, 7, 8, 8.1, 10, 11
Architectures: 32 and 64 bits, builder can generate files for both architectures.
- **No Protected View**
It is always only one click. No need to "Enable Content".
- **Regular updates free of charge**
We regularly check detection status and release updates when they're needed.
- **Professional Support**
If you need assistance - we are ready to help.
Chat, TeamViewer, Anydesk
- **Custom content**
You can insert content of your choice to the document.
- **Attachable on Gmail**
You can attach the XLL to email and send it.
- **Bypass Windows Defender**
This XLL file bypasses Windows Defender Real-time protection and Cloud-protection.
- **Bypass Smart Screen**
If you struggle with Smart Screen blocking your files, then this XLL dropper can be your solution.
- **More information about the features:**
<https://warzone.ws/xll.html>

Figure 6 Malware Dropper with Excel XLL

Purchase of system or software exploits: While many white hats elect to support bug bounty initiatives by vendors, there remains a lucrative underground market for reliable, unpatched exploits

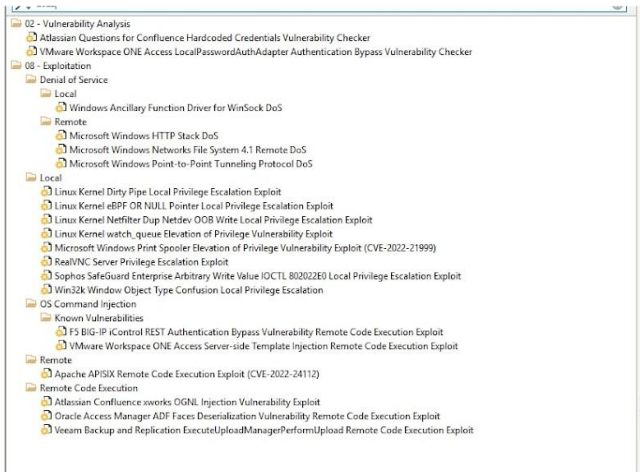
LORD1
terabyte

Posted Tuesday at 03:31 AM (edited)

Exploits for latest vulnerabilities on ongoing basis. All exploits are weaponized and ready for battle conditions. Fully integrated post-exploitation. Easy passing of sessions and newly obtained accesses to Cobalt Strik

Price: from \$10K

Contact with PM.



The screenshot shows a tool interface with a tree view of vulnerabilities. Categories include:

- 02 - Vulnerability Analysis
 - Atlassian Questions for Confluence Hardcoded Credentials Vulnerability Checker
 - VMware Workspace ONE Access LocalPasswordAuthAdapter Authentication Bypass Vulnerability Checker
- 08 - Exploitation
 - Denial of Service
 - Local: Windows Ancillary Function Driver for WinSock DoS
 - Remote: Microsoft Windows HTTP Stack DoS, Microsoft Windows Networks File System 4.1 Remote DoS, Microsoft Windows Point-to-Point Tunneling Protocol DoS
 - Local: Linux Kernel Dirty Pipe Local Privilege Escalation Exploit, Linux Kernel eBPF OR NULL Pointer Local Privilege Escalation Exploit, Linux Kernel Netfilter Dup Netdev OOB Write Local Privilege Escalation Exploit, Linux Kernel watch_queue Elevation of Privilege Vulnerability Exploit, Microsoft Windows Print Spooler Elevation of Privilege Vulnerability Exploit (CVE-2022-21999), RealVNC Server Privilege Escalation Exploit, Sophos SafeGuard Enterprise Arbitrary Write Value IOCTL, 80202ED Local Privilege Escalation Exploit, Win32k Window Object Type Confusion Local Privilege Escalation
 - OS Command Injection
 - Known Vulnerabilities: FS BIG-IP Control REST Authentication Bypass Vulnerability Remote Code Execution Exploit, VMware Workspace ONE Access Server-side Template Injection Remote Code Execution Exploit
 - Remote: Apache APISIX Remote Code Execution Exploit (CVE-2022-24112), Remote Code Execution, Atlassian Confluence xworks OGNL Injection Vulnerability Exploit, Oracle Access Manager ADF Faces Deserialization Vulnerability Remote Code Execution Exploit, Veeam Backup and Replication ExecuteUploadManagerPerformUpload Remote Code Execution Exploit

Alongside with Odays, oftentimes Threat Actors share their experience on widely abused vulnerabilities, this information is so valuable for the Ransomware groups that could help them for mass infection.

VMware Workspace One RCE
By idk, April 12 in Bugtraq

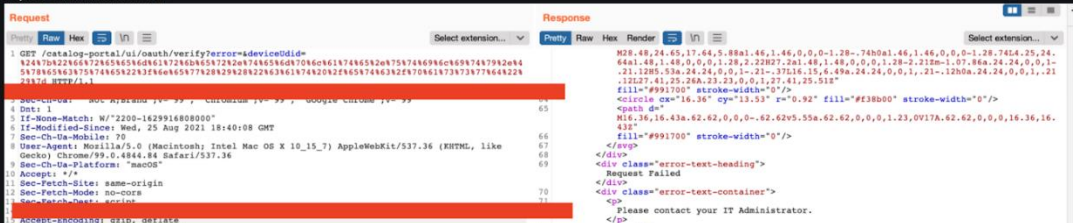
idk
byte

Posted April 12

CVE-2022-22954 with a CVSS score of 9.8: the vulnerability has been described as a server-side template injection remote code execution issue in VMware Workspace ONE Access and Identity Manager. The exploitability is told to be easy. It is possible to launch the attack remotely. The exploitation doesn't require any form of authentication.

<https://github.com/sherlocksecurity/VMware-CVE-2022-22954>

Shodan Query:
http.favicon.hash: 1250474341



The screenshot shows a network traffic analysis tool displaying a request and response. The request is a GET request to a specific endpoint. The response is a 200 OK status with a large body of HTML content, including a script tag that executes a remote command. The response body contains a large block of HTML and JavaScript code, including a script tag that executes a remote command.

Figure 7 VMware Workspace - Remote Code Execution Exploit

Malicious actor training: Guidebooks or tutorials on effective tool usage or specific Tactics, Techniques, and Procedures (TTPs)

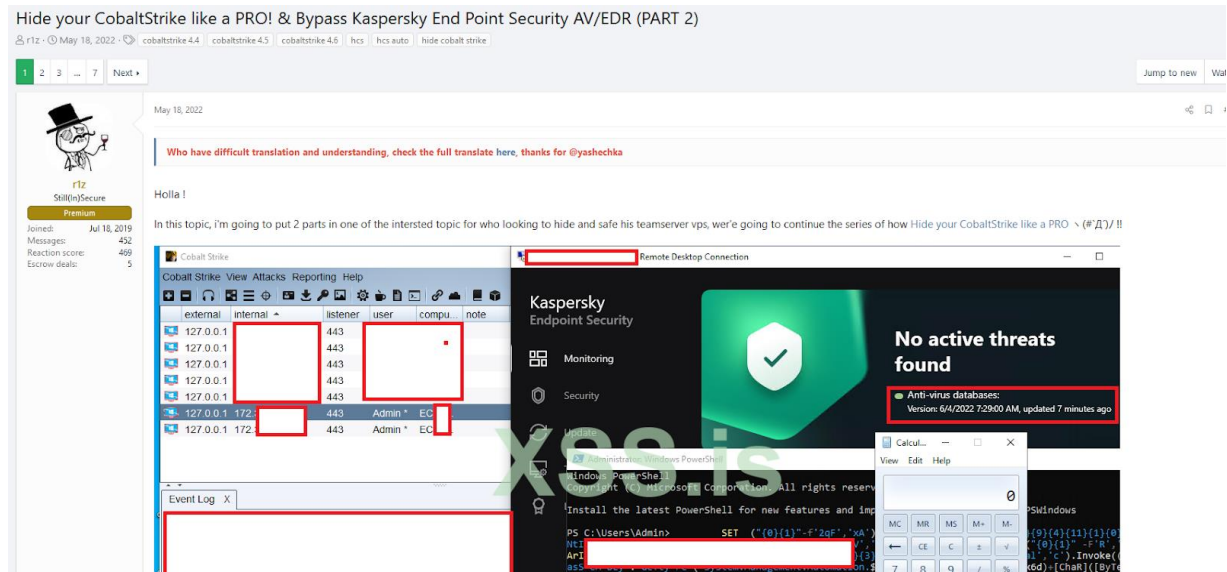


Figure 8 AV/EDR Evasione Techniques

~/ Bypass Kaspersky AV / EDR 04.06.2022

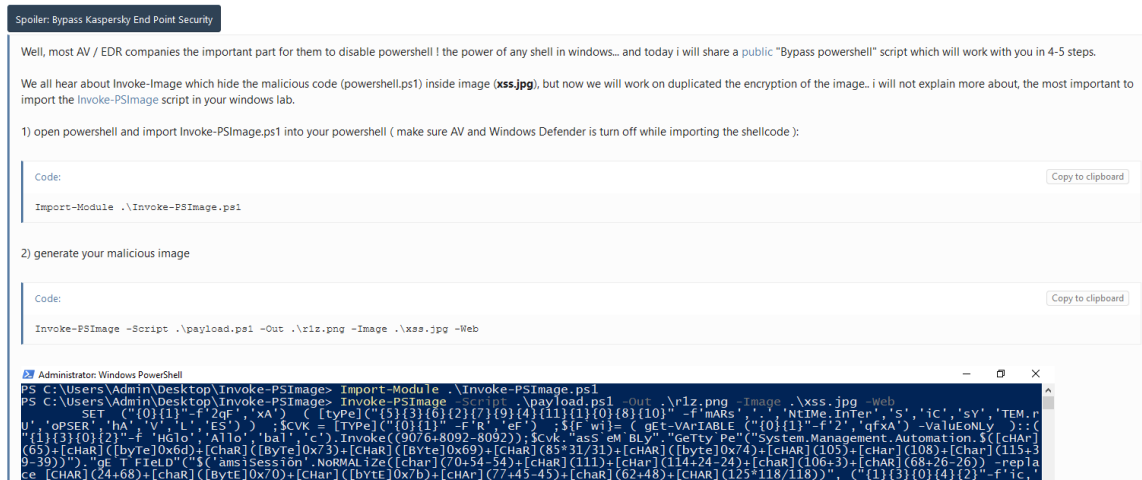


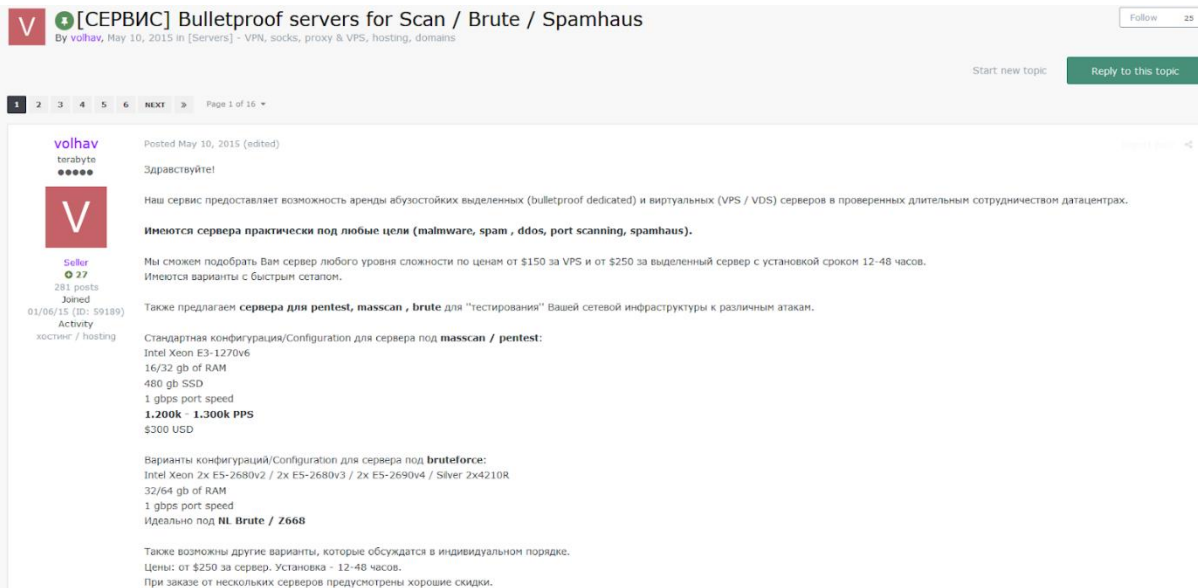
Figure 9 Usage of Invoke-PSImage

Services include the following:

Distributed denial of service (DDoS): These are botnet powered attacks that affect the availability of targeted servers and capabilities.

Exploit kits (EKs): As part of the service offering, exploit kits are typically leased with a monthly rate for access to the exploit toolkit, allowing for customized end payloads.

Infrastructure rental: These include hosting services for attack platforms, malware updates, configuration, command and control (C2), and other attack lifecycle functions.



Money laundering: This is known as the transfer (“Money Muling”) of illegally obtained funds through accounts and mechanisms in money haven countries remains a crucial service.

Initial access brokers: Malicious actors that provide access to secure networks for a fee. They are often hackers but may also gain access to networks using social engineering. Their motivation is not to carry out cyberattacks but rather to sell the access to another party.

Price	IP	Country	ISP	
5\$	99.85.X.X	US	ATT-INTERNET4 - AT&T Services, Inc.	Add to cart
5\$	99.36.X.X	US	ATT-INTERNET4 - AT&T Services, Inc.	Add to cart
5\$	99.247.X.X	CA	ROGERS-CABLE - Rogers Cable Communications Inc.	Add to cart
5\$	98.53.X.X	US	COMCAST-7922 - Comcast Cable Communications, LLC	Add to cart

Figure 10 Wanna buy RDP is the marketplace for the Initial Access, average price for accessing compromised device in US or Canada will cost 5\$

Security strategies for preventing data compromise

Identify and classify sensitive data

Without understanding the sensitivity of data, it is hard to properly secure it. Because of that, companies use Data Classification. Data classification is of great importance for organizations. Purpose refers to the process of analyzing data (both structured and unstructured) and then organizing that data into defined categories based on its content, file type, and other metadata attributes. In this way, a security system that is divided into parts and easier to control is created.

Access control lists

Access control list (ACL) is another form of breach prevention. An access control list (ACL) is a list of rules that specifies which users or systems are granted or denied access to a particular object or system resource.

Each ACL has one or more access control entries (ACEs) that consist of the name of a user or user group. It can also be a role name, such as user, programmer, or tester. Typically, the system administrator or object owner creates the access control list for an object.

Types of access control lists can be divided into two basic items:

File system ACL: Manages access to files and directories. They give operating systems instructions that determine user access permissions and privileges for the system after the system has been accessed.

Networking ACL: Manages network access by providing instructions to network switches and routers that specify the types of traffic they are allowed to interface with the network. These ACLs also specify user permissions once within the network. The network administrator predefines network communication ACL rules. In this way they work similarly to a firewall.

ACLs can also be categorized by the way they describe traffic:

Standard ACL: Blocks or allows an entire protocol packet using source IP addresses.

Extended ACL: Blocks or allows network traffic based on a different set of properties, including source and destination IP addresses and port numbers, as opposed to just the source address.

Data Encryption

Data encryption is very important for internet users. Encryption and protection of private information is very important in today's world where all kinds of information are circulating in the internet world. In this sense, data encryption helps protect private information and sensitive data and aims to increase the security of communication between client applications and servers. In summary, when your data is encrypted, an unauthorized person or organization cannot read it even if it accesses it.

Data encryption is a method of security in which information is encoded and can only be accessed or decrypted by a user with the correct encryption key. Encrypted data, also known as ciphertext, appears to have been scrambled or unreadable by an unauthorized person or organization.

The two most commonly used methods for data encryption are asymmetric encryption and public key, also known as a private key or symmetric encryption. Both are based on key pairs, but they differ in the way sending and receiving parties share keys and manage the encryption/decryption process.

Harden your systems

System hardening is used to reduce vulnerability in technology applications, systems, infrastructure, firmware, and other areas. The purpose of system hardening is to reduce security risk by eliminating potential attack vectors and intensifying the attack surface of the system.

There are several system hardening activities, including:

- Application Hardening
- Operating System Hardening
- Server Hardening
- Database Hardening
- Network Consolidation

Best Practices for Systems Hardening

1. Audit your existing systems: Use penetration testing, vulnerability scanning, configuration management, and other security auditing tools to find flaws in the existing system and prioritize fixes.
2. Create a strategy and plan based on the risks identified in your technology ecosystem and use a phased approach to address the biggest flaws.
3. Fix vulnerabilities now: Make sure you have an automated and comprehensive vulnerability identification and patching system in place.
4. Network hardening: Make sure your firewall is configured properly and all rules are checked regularly.
5. Server hardening: Put all servers in a secure data center.
6. Application hardening: Restrict access to applications based on user roles and context.
7. Database hardening: Create administrative restrictions on what users can do to a database, such as controlling privileged access.
8. OS hardening: Automatically apply OS updates, service packs, and patches.
9. Eliminate unnecessary accounts and privileges: Apply minimal privileges by removing unnecessary accounts and privileges from your IT infrastructure.

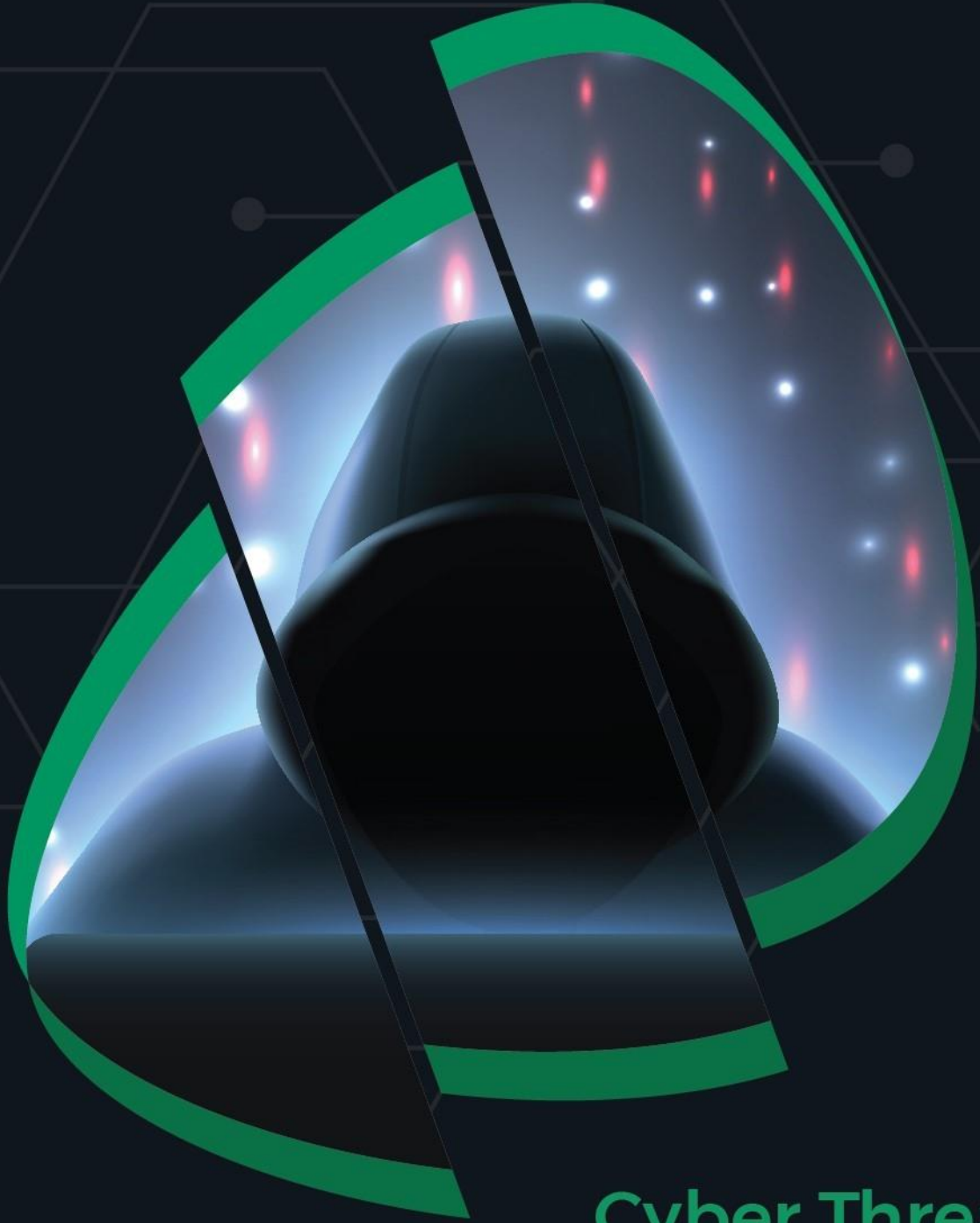
Cyber Security Awareness

First and foremost, a staff well-trained in cyber security poses less of a risk to the overall security of an organization's digital network.

Security awareness training is important as it protects an organization against cyber attacks on the system that result in data breaches. The primary focus is on preventing such incidents that lead to brand reputation and financial losses.

Definitions

- **Cybercrime:** Any crime that involves the use of computers to victimize an individual or organization for financial gain.
- **Deep Web:** Sites that make indexing by Internet search engines problematic, due to access control, dynamic content, or other prerequisite mechanisms (e.g., encryption or specialized software). In general, these sites are not accessible to standard web search engine crawlers that perform indexing. This class of sites is also sometimes referred to as the Invisible Web, Hidden Web, or Deepnet.
- **Dark Web:** A subset of Deep Web sites that requires special software (e.g., TOR) to reach. Related infrastructure hosts criminal content such as stolen information and access to premium malware and exploits, and supports other categories of activity, such as illegal pornography, drug trade, prostitution, human trafficking, and terrorist operations. A number of these sites are transient, only up for a short time or constantly changing addresses in an attempt to minimize the risk of exposure to government agencies, law enforcement and security researchers.
- **Cybercrime underground:** Online forums where information, tools (malware, exploits), and services are bought and sold in support of cybercrime objectives. Composite sites exist on the Indexed Web, Deep Web, and Dark Web in varying contexts.



Cyber Threat
Intelligence:

Dark Web

f |  | in

infinitumitlabs