null NEU

Cyber Threat Intelligence 101

Speaker: Lea Cure

Table Of Contents

01 Intro to Cyber Threat Intelligence

02 Strategic, Operational, Tactical Intel

03 Intelligence Lifecycle

04 The Pyramid of Pain

05 Turning Data into Intelligence

06 Information Sharing Groups

07 Dark Web Research

08 A Day in the Life

09 Resources

whoami

Lea Cure

Cyber Threat Intelligence Manager
Masters in Cyber Security & Intelligence, Digital Forensics
GIAC Defending Advanced Threats (GDAT)

Co-Organizer of Boston Security Meetup
Co-Chair of Women in Cyber
Women in Threat Intelligence

Cyber Threat Intelligence

Cyber Threat Intelligence (CTI) is data that is collected, processed, and analyzed to understand a threat actor's motives, targets, and attack behaviors. Threat intelligence enables us to make faster, more informed, data-backed security decisions and change their behavior from reactive to proactive in the fight against threat actors.

- CrowdStrike

Timely

Actionable

Types of Threat Intelligence

Strategic

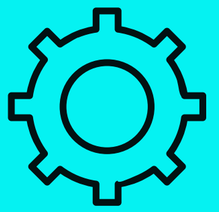
Threat Landscape:
Motivations, Capabilities, Trends

Operational

Immediate Response:
IOCs, Malware Signatures, Attack Patterns,

Tactical

Threat Hunting:
TTPs and Exploit Paths



Intelligence Lifecycle

Phase 1
Scoping Threat Intelligence Requirements

Phase 2
Threat Intelligence Collection

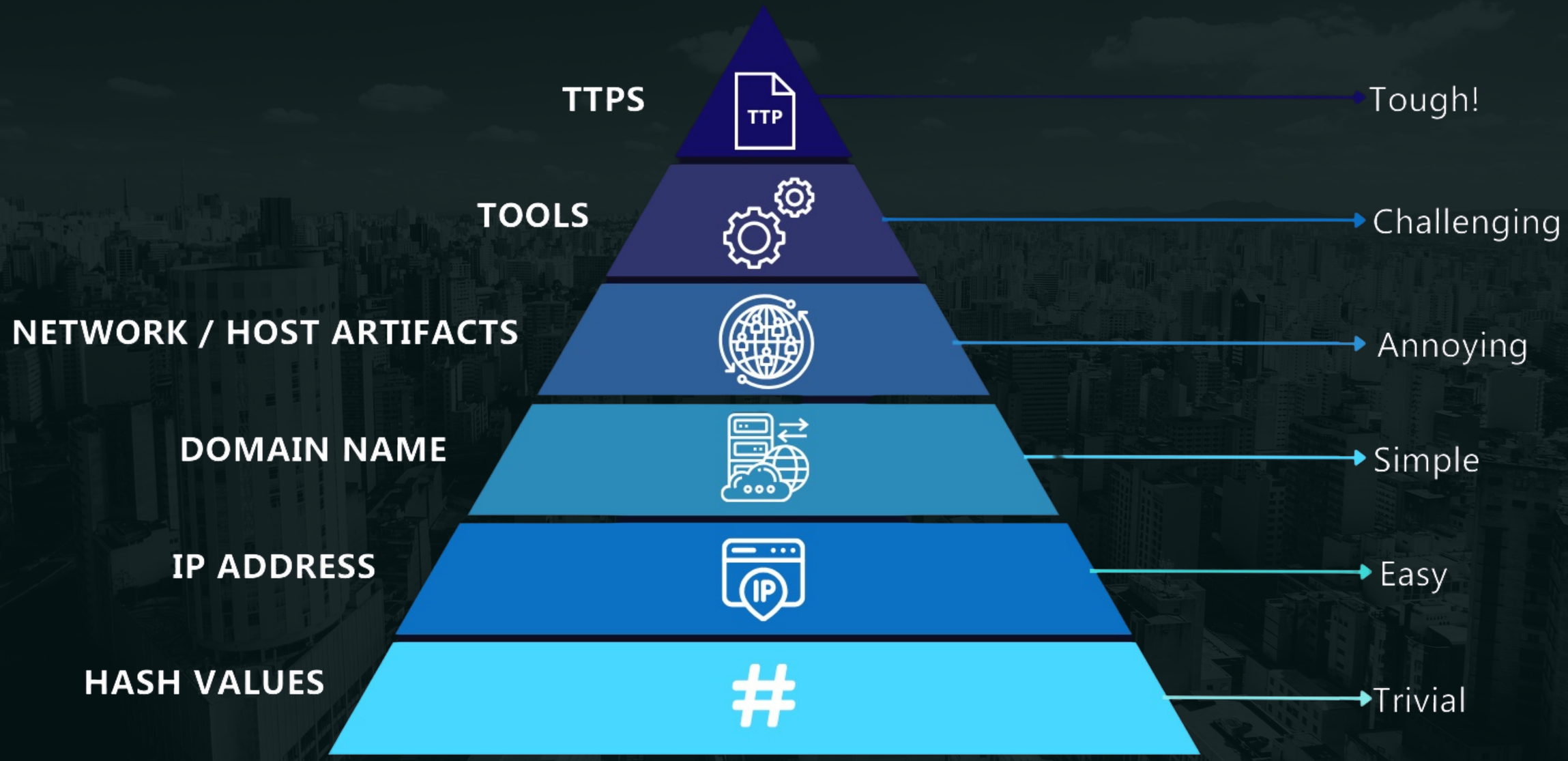
Phase 3
Threat Intelligence Processing

Phase 4
Threat Intelligence Analysis

Phase 5
Threat Intelligence Dissemination

Phase 6
Feedback

The Pyramid of Pain



Turning Data into Intelligence

Data

Collection of data from various sources

Information

Processing the data gathered into contextual information

Intelligence

Analyze and produce finished intelligence using assessments

Decisions

Make informed decisions specifc to the organization based on assessment

Information Sharing Groups - ISACs

Information Sharing and Analysis Centers

Sector-based Information Sharing and Analysis Centers collaborate with each other via the National Council of ISACs.

Formed in 2003, the NCI today comprises 27 organizations. It is a coordinating body designed to maximize information flow across the private sector critical infrastructures and with government.

Dark Web Research

Bank Accounts

I am selling fresh high quality Premium Drops.
I will provide you the fullz for the Bank Drops.
These Bank drops comes with Google Voice Acc.
You will get full account access including answers to secret questions and email access.
This package includes:
Own US HQ MAJOR Bank drop account full online access .
Those bank drops are not hacked or phished, they are created specially for you when you order them.
They are perfect for payment processors (stripe/square/flint etc.)
They are ACH/wire capable.
They are as strong as your own bank account.
FULLS DETAILS (PAST ADDRESSES, RELATIVES, DRIVER LICENCE, DOB, SSN, MMN, ETC.)

PAYMENT PROCESSORS READY
Create and attach any account from Stripe, Square and other payment processors to get money directly into your bank account.
GOOGLE VOICE ENABLED
Bypass any SMS verification with Google Voice phone number enabled and attached to Paypal, Skrill, Coinbase and your checking account.
A fresh number is included in every package.
PAPERLESS STATEMENTS + STEALTH HOME ADRESS
The accounts have complete paperless statements and all online banking features enabled. You are in complete control of the account and the bank will never get in touch of the "real" account holder.
I will provide full instructions on how to keep the account active for up to 4 years.
I can ship visa cards for cashout internationally!

Product	Price	Quantity
Bank account basic	100 USD = 0.00371 B	1 x Buy now
Bank account with verified crypto exchange account	250 USD = 0.00927 B	1 x Buy now
Bank account with VISA card	390 USD = 0.01446 B	1 x Buy now
Bank account with VISA card + verfied crypto exchange account	550 USD = 0.02039 B	1 x Buy now

Fort Financial Credit Union — Contact seller — $140.00 — EugeneK...
- ✅Full Info
- ✅Email Access
- ✅Phone Number(E-sim/Drop Phone Number/Rent sim)
- ✅Online Access
- ✅Driver License (F/B)
- ✅Cookies

PayPal Verified or VCC+AN:... — Contact seller — $80.00 — EugeneK...
- ✅Full Info
- ✅Email Access
- ✅Phone Number(E-sim/Drop Phone Number/Rent sim)
- ✅Online Access
- ✅Cookies

Redline stealer

🔥 I want to present you a stealer designed for convenient work with logs. Collects the most-demanded information for work in all directions. The program was written taking into account all the wishes of people professionally involved in the field of carding.

‼️ Build features:

1) Collects from browsers:
a) Login and passwords
b) Cookies
c) Autocomplete fields
d) Credit cards
2) Supported browsers:
a) All Chromium-based browsers (Even the latest Chrome version)
b) All Gecko-based browsers (Mozilla etc.)
3) Data collection from FTP clients, IM clients
4) Customizable grabber file according to the criteria Path, Extension, Search in subfolders (can be configured for the desired cold wallets, steam, etc.)
5) Sample by country. Setting up a black list of countries where the build will not work
6) Setting up anti-duplicate logs in the panel
7) Collects information about the victim's system:
IP
The country
City
Current user name
HWID
Keyboard layouts
Screenshot
Screen resolution
Operating system
UAC settings
Is the current build running with administrator rights
User agent
Information about the components of the PC (video cards, processors)
Installed antiviruses
8) Completion of tasks:
a) Download - download a file via a direct link to the specified path
b) RunPE - inject a 32-bit file downloaded from a direct link into another file that you specify
c) DownloadAndEx - downloading a file via a direct link to the specified path with subsequent launch
d) OpenLink - open link in default browser

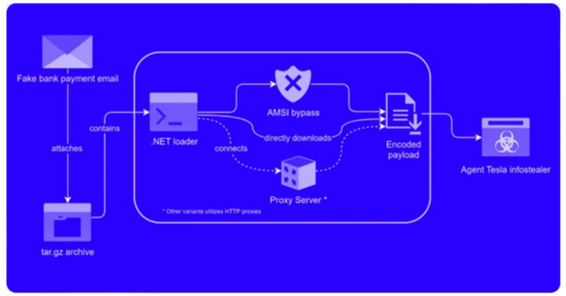
A day in the life of a CTI analyst

#1 Trusted Cybersecurity News Platform

The Hacker News

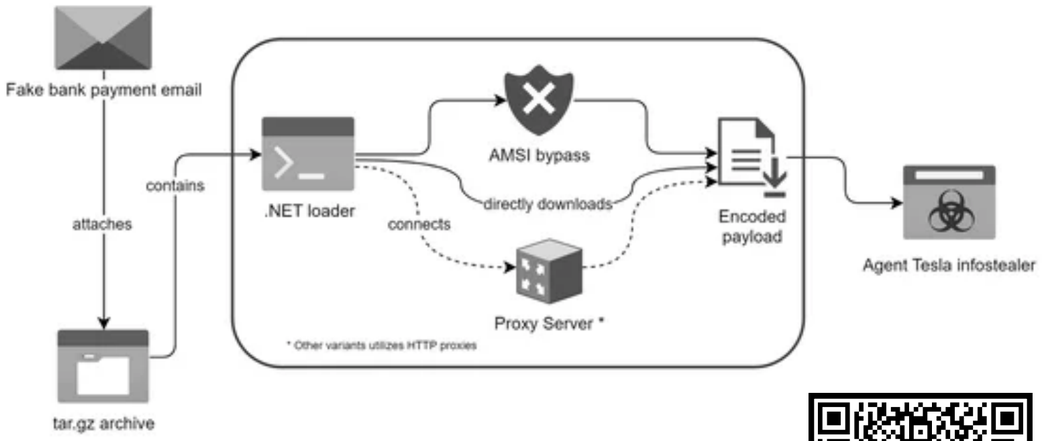
Home | Newsletter | Webinars

Alert: New Phishing Attack Delivers Keylogger Disguised as Bank Payment Notice



Mar 27, 2024 Vulnerability / Cybercrime

A new phishing campaign has been observed leveraging a novel loader malware to deliver an information stealer and keylogger called Agent Tesla ...



Indicators of Compromise

Loader (Variant 1)

MD5 b69f65b999db695b27910689b7ed5cf0

SHA256 ab9cd59d789e6c7841b9d28689743e700d492b5fae1606f184889cc7e6acadcc

Loader (Variant 2)

MD538d6ebb40197248bc9149adeec8bd0e7

SHA256a02388b5c352f13334f30244e9eedac3384bc2bf475d8bc667b0ce497769cc6a

New Sources

The Hacker News

Bleeping Computer

The Record

ZDNet

Podcasts

Click Here

Dark Net Diaries

The Cyber Wire

Wired Security

Tools and Resources

CTI Sources

CTI Tools

OSINT Sources

Questions?

Add me on LinkedIn!