CYBER INTELLIGENCE REPORT

Q1-2020

BY

INFORMATION WARFARE CENTER

IN PARTNERSHIP WITH

netSecurity

SOCRANGE

LINUX

DIVE INTO THE 5TH DOMAIN THREAT INTELLIGENCE

Join us on our group where "Pls can u hack facebook?" questions are not allowed
https://www.facebook.com/groups/cybersecrets/

Table of Contents

What is inside 1

Cyber Attacks Can Kill 1

Dark Web Corner

- **Kilos: The Dark Market Search Engine** 2
- **Facebook's Tor Hidden Service** 2
- **Dark Market Exit Scams** 3

OSINT Investigations

- **Online and Dark Web Investigations: CSI Linux** 2
- **OSINT & Online Investigation Tips** 5

Tools and Tips 5

Human Trafficking & Missing Persons 6

Shadowdragon Dossier Template 7

CSI Linux Forensic Challenge 8

Chain of Custody Template 10

Different levels of data destruction & recoverability 12

Security Vs. Privacy 16

Anonymity on the Web: Installation and Configuration of Tor and Privoxy 29

OSINT Reconnaissance: An overview of OSINT with Recon-ng walkthrough 44

Digital Forensics & Incident Response

- **Introduction to Digital Forensics and Autopsy Installation** 64
- **Elastic Stack with Zeek (Bro) IDS Integration** 75
- **Configuring Zeek (Bro) IDS Signatures** 130

Sponsors

- **SOC Range ®** 153
- **ThreatResponder ®** 154
- **CSI Linux** 155

Credits 156

Information Warfare Center Projects 157

Copyright 157

Disclaimer: **Do NOT break the law!**

While every effort has been made to ensure the high quality of the magazine, the editors make no warranty, express or implied, concerning the results of content usage.

When accessing Dark Web sites or any site linked in content referenced in Information Warfare Center, LLC publications, websites, or resources, you are doing so at your own risk. ***To access .onion sites, you must have access to the Tor network. To access i2p sites, you must have access to the I2P network. To access any Surface Web site, you must have access to the Internet.***

What is inside?

The Cyber Intelligence Report (CIR) is an Open Source Intelligence (***AKA OSINT***) resource focusing on subjects such as Advanced Persistent Threats, National Infrastructures, Dark Webs, and other digital dangers.

This publication focuses on educational items with articles and hands on walkthroughs of subjects ranging from exploit development to Digital Forensics and Incident Response (DFIR).

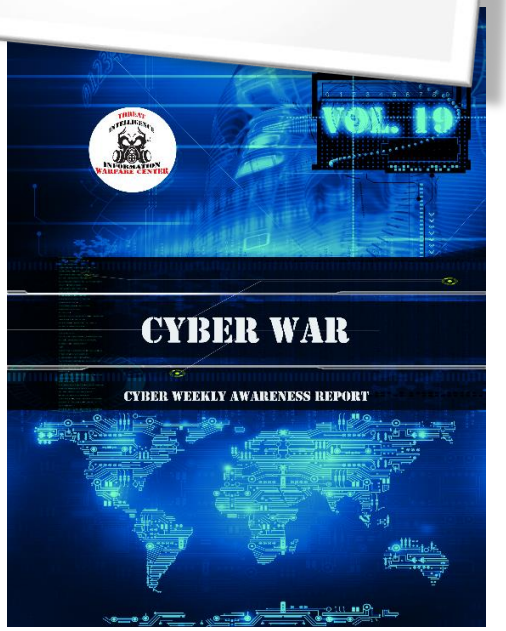
InformationWarfareCenter.com

Many of the articles and walkthroughs in the CIR are part of our online security training solutions at:

Academy.InformationWarfareCenter.com

Articles that focus on cyber defense and investigation usually spotlight capabilities that are or will be included in the CSI Linux distribution. If you are interested in helping with the project, please let us know.

csilinux.com



CYBER WAR

Weekly Awareness Report

We have another publication called the Cyber WAR. It contains information pulled from many different sources to keep you up to date with what is going on in the Cyber Security Realm. You can read past Cyber WAR editions at:

InformationWarfareCenter.com/CIR

"Hospitals that have been hit by a data breach or ransomware attack can expect to see an increase in the death rate among heart patients in the following months or years because of cybersecurity remediation efforts, a new study posits. Health industry experts say the findings should prompt a larger review of how security - or the lack thereof - may be impacting patient outcomes." – Krebsonsecurity.com

Cyber Attacks Can Kill

Ransomware has cost both business and individuals billions of dollars and an untold number of hours causing damages far beyond what most people can fathom. Researchers at Vanderbilt University identified a pattern that ties cyber-attacks to medical patient mortality.

Heart attack deaths increase…

Adding the additional stress of a cyber-attack with an overwhelmed staff that can't get access to patient data; care goes down while mistakes go up. These are just the tip of the iceberg when it concerns how a digital assault can turn deadly. Here are examples of how the digital world can physically affect the real world.

* The Russian cyber-attack against the Ukrainian energy grid in 2017 attempted to cause a fatal disaster.

* Targeting medical equipment with wireless or network access can easily turn grave. Think pacemakers…

* Exploiting vehicles, drones, and autonomous machines can become effective kinetic projectiles. Makes a bad day for all those involved.

* After the data breach of the site Ashley Madison, there were several alleged suicides.

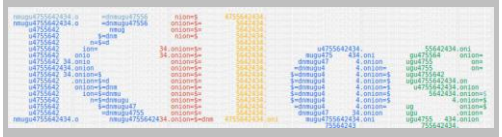
Where do you start to investigate these types of crimes? This is where OSINT investigations come into play and may help identify the suspect(s).

DARK WEB CORNER

Kilos Dark Market Search Engine

About Kilos

As per this article, Kilos was searching over 525k forum posts, 60k listings, 2500 vendors, and 190k reviews of 5 of the biggest Tor Dark Markets.



Dnmugu4755642434.onion

Facebook Tor Hidden Service

"**facebookcorewwwi.onion** is a site that allows access to Facebook through the Tor protocol, using its .onion top-level domain. In April 2016, it had been used by over 1 million people monthly, up from 525,000 in 2015. Neither Twitter nor Google operate sites through Tor, and Facebook has been applauded for allowing such access, which makes it available in countries that actively try to block Facebook." …

"Prior to the release of an official .onion domain, accessing Facebook through Tor would sometimes lead to error messages and inability to access the website. There are numerous reasons to use the Tor-protocol for legitimate purposes, such as for increased anonymity when connecting to Facebook. ProPublica explicitly referenced the existence of Facebook's .onion site when they started their own onion service."

facebookcorewwwi.onion

FUN FACTS

75%

Of the close to 200 domains catalogued as illegal by Terbium Labs, more than 75 percent appear to be marketplaces:

Online and Dark Web Investigations:
CSI Linux based investigations

Social Media, Dark Markets, and other online investigations are probably some of the most challenging types to start because technology, laws, and trends change on what seems like a daily basis. Figuring out where to even start these investigations can even be a daunting task. If this field was easy, everyone would be doing it.

Hackers use similar tools and techniques; they just have a different endgame. The term "*two sides of the same coin*" comes up often when discussing both the hacking and investigation sides of cyber.

There are a ton of tools out there that you can use to track people, recon a business, or even see if your personal information has been leaked on the Internet. Some tools can be very expensive to license. With so many resources out there, a lot of people do not know where to start.

Some of this becomes a little easier with the release of CSI Linux on January 1st, 2020.

This environment was built with investigators in mind. It contains some of the more well-known tools along with a set of custom tools to standardize your evidence gathering and manage your case files.

The inaugural release comes in a VirtualBox appliance (***CSI Linux Investigator***) to make it as simple as possible to install and use.

CSI Linux Investigator contains all 3 of the CSI Linux VirtualBox appliance in an OVA package. When you download this, it will automatically setup and load them into VirtualBox.

You must install VirtualBox first, install the VirtualBox Extension Pack, then run the downloaded OVA file. The OVA file contains:

- ***CSI Linux Analyst***
- ***CSI Linux Gateway***
- ***CSI Linux SIEM***

CSI Linux Analyst is the main investigation workstation that is used for digital forensics and contains the tools to investigate, capture, analyze, and report. Keep in mind, some tools required API keys. These keys can be free while others require licensing to unlock their full potential.

CSI Linux Gateway is required to send all CSI Linux Analyst traffic through Tor and hide the source IP addresses. It protects all the analyst's traffic through a Tor Proxy to provide additional safety while allowing the analyst to use most of your surface web tools on the Tor Dark Web.

CSI Linux SIEM is used for Incident Response and Intrusion Detection. This can be used as a stand alone or with CSI Linux Analyst for a more indepth analysis. It offers machine learning, intrusion/Tor detection, and other incident response capability. Some of the muscle under the hood consists of Elasticsearch, Logstash, Kibana, and Zeek IDS.

When using the CSI Linux Gateway, one hurdle you may come across is piping through Tor. Many sites now force users exiting the Tor network to complete a CAPTCHA which prevents automated tools from working as well. Tor also doesn't work exactly like the Internet when it comes to networking, making it difficult to use some tools for reconnaissance. This environment has a few alternatives that help maximize your ability while minimizing your cost and efforts.

In this modular approach makes this environment a scalable solution for an analyst or a team of investigators.

With the inclusion of a case development feature, an analyst or investigator can manage their case more easily. Prebuilds a structured case folder for your evidence capture, hashes all case files, and makes a forensic archive of the case for distribution.

Some of the features that are within this functionality include:

- Username search
- Adult website username search
- Twitter information gathering
- Domain reconnaissance
- Website link extraction
- Website forensic imaging
- Website page snapshot (image)
- Website “de-clouding”
- Bitcoin wallet lookup
- Android/iPhone forensics

The list goes on and is growing...

The CSI Linux Investigator was built for ease of use and to give an extra layer of anonymity while investigating, along with a SIEM solution for security and incident response. This includes 3 systems in 1 appliance.

With this design, each component can be used independently, in pieces, or all together.

Scenarios

What can you use this environment for? Here is a list of scenarios and the systems to be used in each:

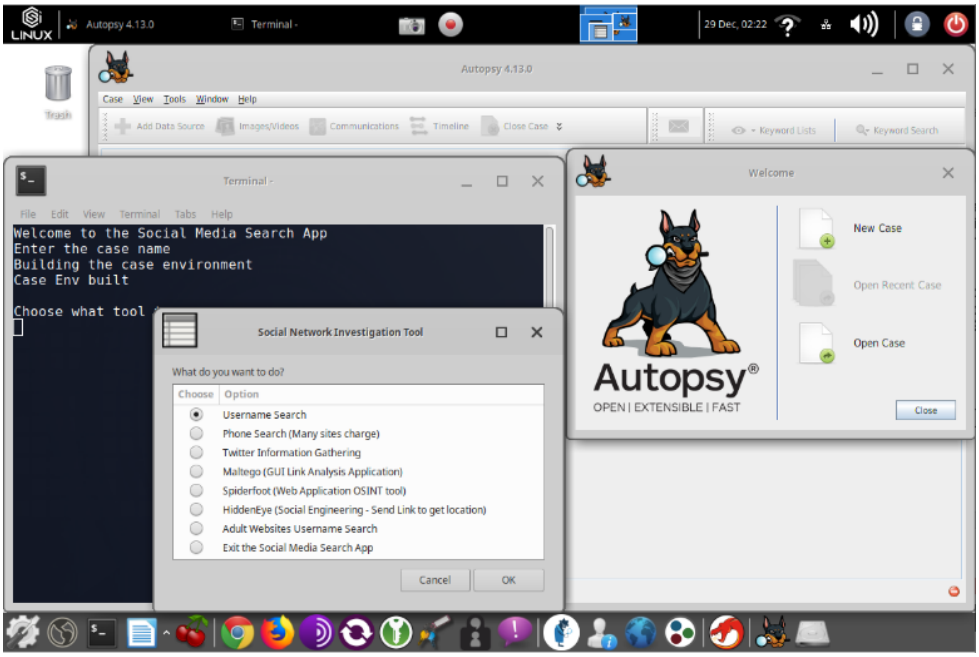
#1: Online Investigation.

CSI Linux Analyst

You know the suspects username, but you don’t know where they are located. Many people will reuse their username because it is comfortable to them. It is like a “signature”, brand”, or “trademark” of themselves. In this instance, you want to identify as many sites as you can that may have information related to where the suspect is, but you don’t care about protecting your location. You can use:

- CSI Tools “Social Media Search” to search for usernames over many different websites: UsernameSearch / AdultUsernameSearch.
- Hunchly plugin for Google Chrome to record your activity and findings.
- EyeWitness to screen capture a specific page on the website in question
- Maltego for link analysis.
- You can also use the Linux screen capture tool or RecordMyDesktop.

Use the SocialDragon Dossier template to fill in your findings to make a sharp looking report.



#2: Undercover work.

CSI Linux Analyst
CS Linux Gateway

The suspect is in an alleged Internet piracy group. You do not know their name, location, or anything other than a forum you know they post content on. You want to hide your location along with being able to use Tor for communications.

This type of investigation would require a few basic tools, but also the software that the suspect group is using as well. VPNs do not really mask your data because they are only behind one hop. This means that if the VPN service or your system gets compromised, you are more likely to leak your real location.

Using the CSI Linux Gateway allows you to add a local layer of security along with the obfuscation of the Tor onion routing network. All of your tools are also going through Tor, giving access to “.onion” domains.

You can use KeepPass to keep your undercover persona stored, OnionShare for securely sharing files, and the communication protocol of choice like Pidgin or qTox.

Maltego fits with every kind of investigation by providing link analysis and additional search capability in the form of “Transforms”.

#3: Incident response.

CSI Linux SIEM
CSI Linux Analyst

The network has been compromised and you suspect the hackers may still be on the systems. You need visibility of what is going on.

With Zeek (Bro) IDS in place, using custom signatures and Filebeat sending key indicators to Logstash, Kibana uses Elasticsearch to to give actional information in an easy to view dashboard.