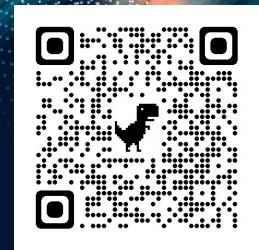


Slips



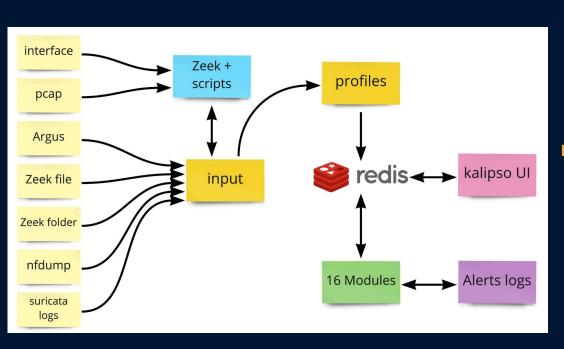
A Machine-Learning Based, Free-Software, Network Intrusion Prevention System

Alya Gomaa, Sebastian Garcia

What is Slips

- Intrusion Prevention System
 - Uses iptables in Linux to block attackers automatically
- Designed for endpoint devices
- Behavioral detection
 - Detects attacks based on their behavior
- Machine Learning
 - Together with an ensembling algorithm
 - Models are open source

Slips Architecture



Profiles

- Create profiles for devices
- Time windows analysis
- All traffic in and out is analyzed

Top Features

- Behavioral time-based rules for detection of infections
- Machine Learning detections
- Ensembling evidences in Alerts
- P2P
- Modularity for new functionality
- Whitelists for organisations

Slips local P2P network

- A module that creates and maintains a local P2P network.
- Slips Peers find each other automatically using multicast.
- Slips peers can:
 - Ask other peer what they think about an IoC
 - Receive requests for opinion about an IoC
 - Send alerts for IoC that should were detected to the network
- Trust Model to be resilient against adversarial peers



See Slips in Action!

How Slips detects problems in the network

All Slips features 1/2

Daemon Mode

Simultaneous Slips Zeek logs rotation

Automatic management of Redis DB Local P2P network Detect young domains

Detect bad SMTP logins Detect SMTP bruteforce

Detect DNS ARPA scans Multiple SSH versions

VirusTotal

Check IPs, domains, URLs

Detect DNS without resolution

Detect empty HTTP connectivity checks to google.com, Yandex and bing.com Detect ICMP scans

Timestamp
 Netmask

· Echo request

Whitelist

- IPs, domains, MACs, organisations names
- Whitelist flows or alerts
- Search on flows IPs, TLS SNI, DNS query and answer, HTTP host.
- Organisation names use:
 - List of IPs, domains and
 ASN

Detect DoH flows

Get geolocation of IP

Detect vertical and horizontal port scans

Detect malicious flows by ML

Detect SSH bruteforce

Get RDNS of IPs

Threat Intelligence

- Download 45 lists from the Internet
 Ensemble the lists
 - · Update the lists periodically
 - Custom local lists
 Feeds confidence and threat level
 - · Feeds have tags, like 'honeypot'
 - · Get known list of TOR exit nodes

Get the

Detect Connections without DNS

 Dont alert on IPs of well known organisations Generate notification popups in linux and MaCOS C&C channels detection by ML

Detect long connections

Download JA3 feeds

Download malicious TLS cert feeds Detect connection to port 0 Detect multiple reconnection attempts

Detect self signed certificates

Detect invalid SSL certificates

Detect data exfiltration

Generate json alerts in IDEA0 format

All Slips features 2/2

· Custom list of special ports used Get MAC vendor Track special Detect Detect Use RiskIQ by each application Compare MAC vendor of device · Phishing domains incompatible online and ports used by OS · Spotify ports connection to - macos ports with user agents found in its TLS feed API offline and apps user agents http traffic multiple ports · Passive DNS query IRC analysis Detect multiple Detect Custom ARP detection Save and · Don't alert for ports that appear Detect different UA DoH detection user agents in Detect DGA connections to in an FTP connection Detect if the UA belong to · ICMP scans Load the DB Zeek scripts · Don't alert P2P ports HTTP unknown ports different OS (macos, linux, win) Add IA3S Add ja3 · Check valid certs Send alerts to Compatible Check ARP Export alerts YARA GPS Format of export CESNET · Suricata ISON with logstash to remote IP to Slack alerts logs · IDEA0 ISON leak detection Have custom YARA rules WARDEN · TXT Detect Web Build profile Detect malicious Detect MITM Kalipso nodeis Get device type, browser suspicious user downloaded files and OS info from user Detect gratuitous ARP of each IP interface interface attacks agents found in HTTP Detect ARP scans agents from lists using VT traffic Suricata files Detect ARP Multiple nfdump Export alerts to Detect Detect SSH · Zeek folders and conn.log · Detected by Zeek outside local successful access · Detected by Slips unsolicited ARP TAXII servers inputs interface network · Argus

THANKS!

Alya Gomaa alyaggomaa@gmail.com @coreflood_ Sebastian Garcia eldraco@gmail.com @eldracote

https://github.com/stratosphereips/StratosphereLinuxIPS

Documentation:

https://stratospherelinuxips.readthedocs.io/en/develop/.

Slides: https://bit.ly/BHUSSlips2022

CREDITS: This presentation template was created by Slidesgo, including icons by Flaticon, and infographics & images by Freepik.

Example of GPS leak detection

. Detected NETWORK gps

1970-01-01T00:56:31.946939+00:00: Src IP 10.0.2.15 (TINY71)

```
location leaked to destination address: 172.217.18.174 AS: GOOGLE, US AS15169 SNI:
www.google-analytics.com, rDNS: fra15s29-in-f14.1e100.net port: 80/tcp http. Leaked location:
11=48.850113,2.306764
1970-01-01 01:56:31.946939 IP 10.0.2.15.51217 > 172.217.18.174.80: Flags [P]
E...%.@....
  Host: maps.google.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:53.0) Gecko/20100101 Firefox/53.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.unesco.org/new/en/unesco/about-us/where-we-are/visit-us/
Cookie: NID=102=CgWrVrywC3uFGNLitTaINFmAgYWMxK5DwDggl0X93bQYXBRG3XvUYfK5iaeif
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```